PERFORMANCE WORK STATEMENT

A procurement by the
U.S. General Services Administration
Region 5 Contracting Division

on behalf of

CLIENT AGENCY:
General Services Administration (GSA) Office of the Chief Information Officer

PROJECT TITLE:
FAS Cloud Services Support

PROJECT NUMBERS:
47QDCB22K0004

This requirement is being solicited as a Task Order under the

NAICS 541519 – Other Computer Related Services
Product Service Code DA01 – IT and Telecom – Business Application/Application Development Support Services (Labor)

ORIGINAL VERSION DATED
02 February 2022

Post Award Document Revision History

Revision Number	Description of Changes	Requested By	Date

Contents

Contents

1. INTRODUCTION

1.1 a Requiring Organization Mission

This procurement is being conducted on behalf of the GSA Office of the Chief Information Officer, Office of Acquisition IT Services, 1800 F St., NW, Washington, DC 20405. Its mission is to provide the organization with a focused portfolio of applications that enable GSA to meet growth objectives in an agile, efficient timeline, without unintended consequences. The OCIO for Acquisition IT Services provides GSA with strategic and tactical IT business solutions to enable GSA to effectively serve its customers, who are primarily other government agencies. The IT solutions must align with the business portfolio's needs and mission to be effective. And they must be flexible enough to support the changing business environment.

As part of this overall mission, GSA has established a program for transitioning business applications from legacy servers to the Cloud. The Cloud Integration Shared Services (CISS) and FAS Cloud Services (FCS) (referred to as "Program") currently supports 60+ discrete tenants (GSA business units) whose IT requirements are of various size and complexity. The Program provides cloud advisory services, shared cloud services, deployment of immutable application workloads, storage and access of reporting data, and foundations for prototype development in a cloud environment.

The Program supports agency-wide cloud integration through CloudAdvocacy, Advisory, and Enablement coordinating with each tenant and partner to ensure business objectives, technical requirements, reuse services, budgets, schedules, and otherconsiderations are accounted for and mutually understood and set up for success. These groups, along with the FCS product teams, support the organization and business, to include leadership, tenants, strategic partners, product owners, product teams and stakeholders providing coordination, prioritization and scheduling of resources to ensure development, analysis or deployment remains on schedule and in line with the current strategies and future directions of products and services.

1.1 b Tenants & Business Systems Supported

A number of tenants have completed their initial cloud journey, laid out within the IT Playbook, having had their information technology business applications progress from Strategy, through Planning, and Adoption to Optimization while other tenants are in the beginning stages of establishing their business objectives and cloud strategy. Existing tenants will come through the cloud advisory and enablement process when they wish to establish their cloud modernization strategy or when they anticipate a significant change or adjustment to their Applications usage of cloud capabilities.

Over the next five years the volume of work in Technical Objectives 1, 2, and 3 is expected to increase over the previous year by the percentage as shown in the

following table as GSA tenant organizations move their applications to the cloud. As-Need Support (Objective 4) is projected to increase based on the ceiling amounts entered in the price schedule by the Government.

5 Year Program Adoption Growth					
	Base Year	OY1 Growth	OY2 Growth	OY3 Growth	OY4 Growth
Labor (Mandatory)	$25M +/- 5%	39.12%	32.69%	33.90%	33.90%

Cloud Tenant Roadmap - Figure 4.12

1.2 Procurement Objective

The Government's procurement object is to award a task order under the COMET Blanket Purchase Agreement to a highly capable company who will help CISS and FCS engineer and support services and solutions that enable the modernization and transformation efforts of GSA portfolios of systems and applications. Through close partnering and collaboration CISS, FCS, and the Business System teams align with and continue to build on the IT Playbook utilizing standardization and reuse principals to grow the FCS EcoSystem. The Program has an array of functional responsibilities that include focus areas such as Cloud Leadership, Cloud Advisory and Enablement, Cloud Services, and Cloud Support for stakeholders to execute their business operations effectively and efficiently.

This task order is structured to support GSA IT enterprise-wide cloud computing environments that develop and maintain information technology systems and applications, while executing strategic goals and priorities of the GSA IT organization. A major function of the Program is resource planning and sharing with a systematic purpose to make the

organization more efficient and to save GSA money by reducing repetitive work and purchases that could maximized via shared services, shared data, and/or shared systems.

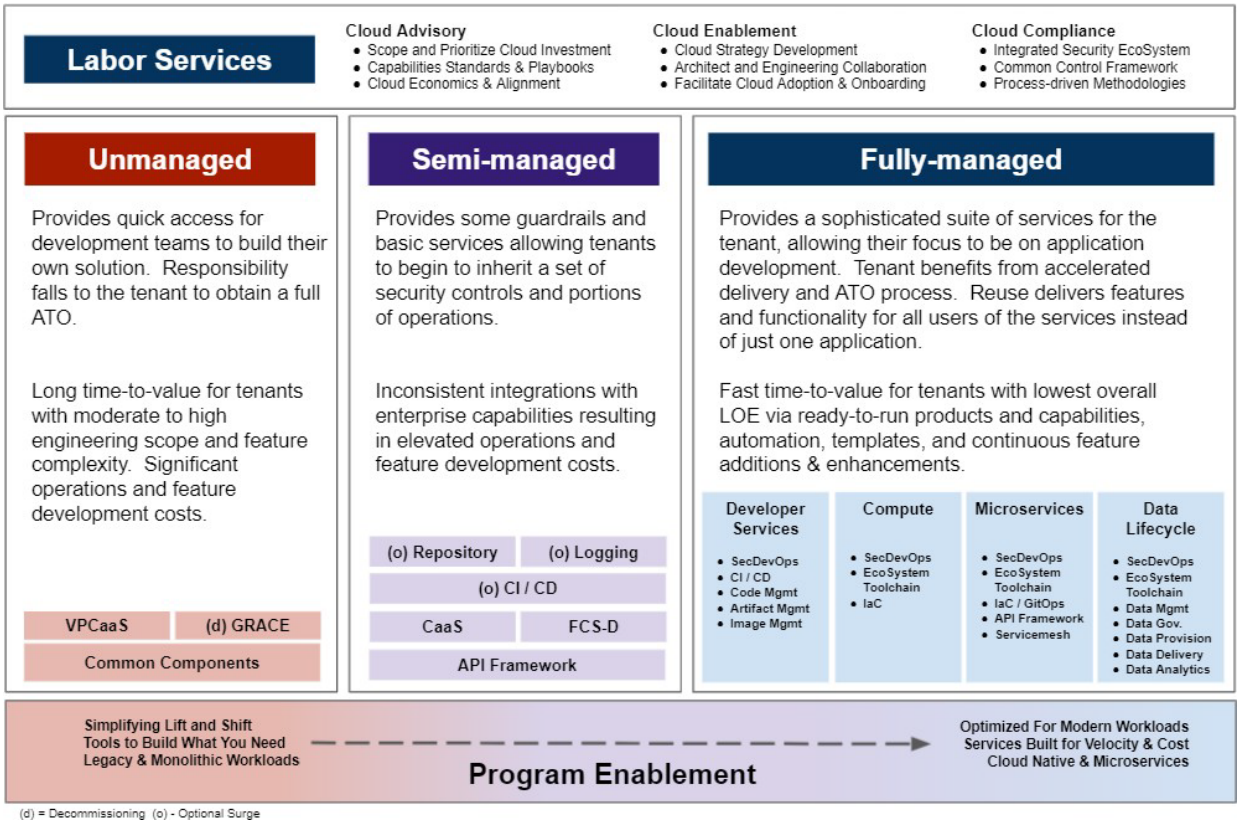
1.3 Scope

Within this section the government is providing an overview of the key considerations of the current cloud services EcoSystem to include core products,–services, and operating procedures supported today. This section is intended to orient the reader with therough scope and approach to operating and maintaining the Program. Additionally, this current orientation, in combination with select optional task objectives, is intended to help the contractor in proposing areas of possible improvements and innovation aspart of establishing a multi-year roadmap for invest, refactor, maintain, or decommission.

This Performance Work Statement (PWS) defines selected acquisition, and program support objectives for the Program. This work to engineer and support services and solutions that ultimately enable the modernization efforts of the FAS portfolio of applications. This contract is intended to provide an array of functional areas that include standardizing, acquiring, engineering, securing, delivering, and maintaining software and cloud services for its FAS business stakeholders to effectively enable them to conduct operations. Work will be performed over a period of five years, with an anticipated Base Period of 12 months and 4 Option Periods of 12 months each.

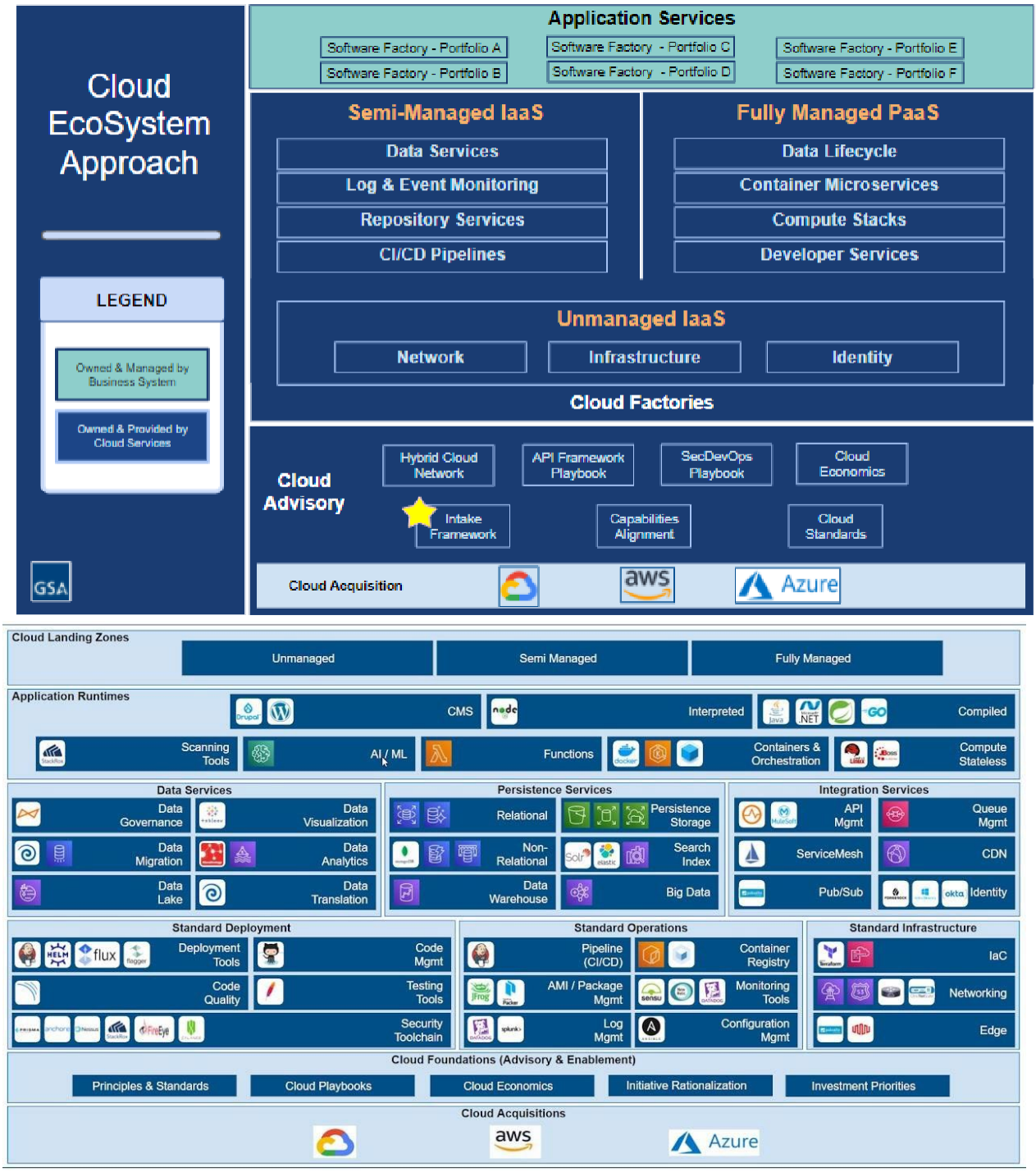
1.3.1 Cloud Services EcoSystem

The direction, in terms of architecture, implementation, delivery, and services of the Program will align with that of the overall GSA IT. It will be very common for teams to participate in the Cloud Enablement process to develop “road-map” architectures as part of their cloud strategy. This will ensure that all stakeholders can anticipate changes over time, giving the business and IT a chance to plan for the future. This EcoSystem approach is prudent and allows teams to re-engage in the Cloud Enablement process when they anticipate major changes and/or upgrades to their system architecture to ensure standardization and reuse are delivering maximum value.



Cloud Services - Figure 4.4

Currently the Services outlined within Figure 4.4 are supported as independent products within the cloud services portfolio. As the program continues to mature the government envisions these services maturing into complementary and more closely connected landing zones that will themselves be built and rely on reuse from each other, supporting an iterative transformation, if necessary, from Unmanaged to Semi-managed and ultimately to Fully-managed. Within this section you will find additional details to the key services supported today within FCS. While this is not an exhaustive list, it represents a large portion of the cloud portfolio.



Cloud EcoSystem Approach - Figure 4.5

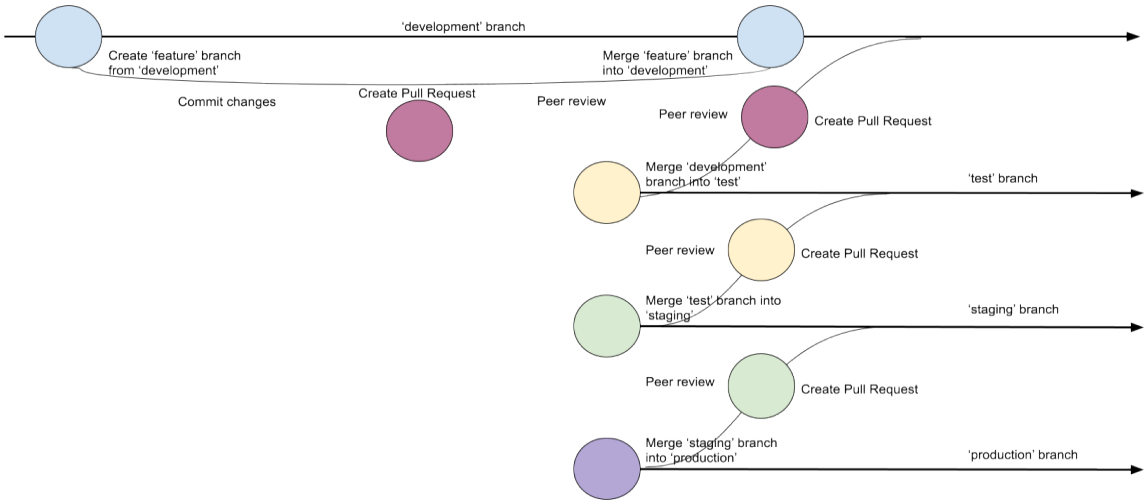
Figure 4.5, represented further within the IT Playbook / Cloud Services as well as the Appendix A - Inventory tab, provides a conceptual example of a products/services architecture with common, modular, and loosely coupled components utilized to meet the evolving mission needs of the business systems. It is key for the EcoSystem to remain relevant and for the Program to stay aware and educate tenants that the cloud is

a developing and changing target, therefore we must all recognize the need to change with it as it matures.

1.3.2 EcoSystem GitOps

The Program adopted the GitOps paradigm and requires all members who work with the program to have an excellent knowledge and skill in this technique. This focus on codebase to manage the services and products, resulted in frequent measurable changes that provide the auditability and change control the program requires.

All technologies within the program follow the GitOps process.



Cloud EcoSystem GitOps- Figure 4.6

1.3.3 Multi-tenant Containers as a Service (MCaaS)

Containerized application designs provide several benefits vs other methods such as virtualization. This type of isolation has become a main design for increased portability and higher level functions that are managed via an orchestrator (upgrades, rollback, health check, etc.). MCaaS provides the application teams the mechanism to adopt this method of development and use secure tooling to deliver business features within this EcoSystem.

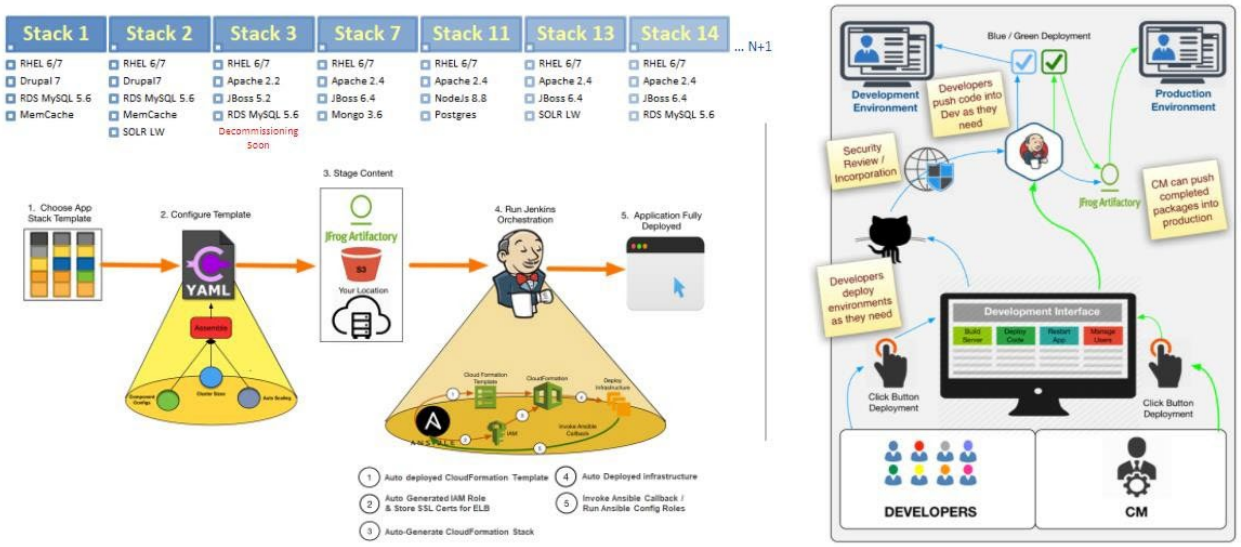
FCS MCaaS Capabilities - Figure 4.7

MCaaS has built-in security compliance in all the environments. This incorporates the baseline so GSA Security can focus reviews on only the area of responsibility of the application features. MCaaS also has native integration with other FCS services (IDM, CI/CD, GitHub, Artifactory, Splunk, DataDog, etc.). Elevated observability for distributed application workload (APM, dashboard, distributed API tracking etc.). MCaaS does not require the application team to maintain any of the infrastructure, such as patching or security compliance.

1.3.4 Everything But The App (EBTA)

EBTA is a hosted environment offering pre-configured application stacks that are made up of system components. The components include the Operating System, Middleware, Database and Web components. EBTA offers a variety of preconfigured stacks that FCS Tenants can use.

EBTA functions solely through the use of CI/CD capabilities which automate the infrastructure environment allowing rapid deployment of applications in minutes.



FCS EBTA Services - Figure 4.8

1.3.5 FCS Data (FCS-D)

FCS-Data services are the technical execution of the FAS (Federal Acquisition Service) Data sources which serves the organization of FAS and enforces the FAS' Data Governance policies/practices. FCS-Data operationalizes the engagement, migration, processing and securing of all FAS business data within FISMA moderate security boundary and maintains enforcement of data classification and roles/relationships with data. The outcome of the data services is to provide the capabilities (tools and processes) for the FAS Data's Business Model(s) to evolve continuously.

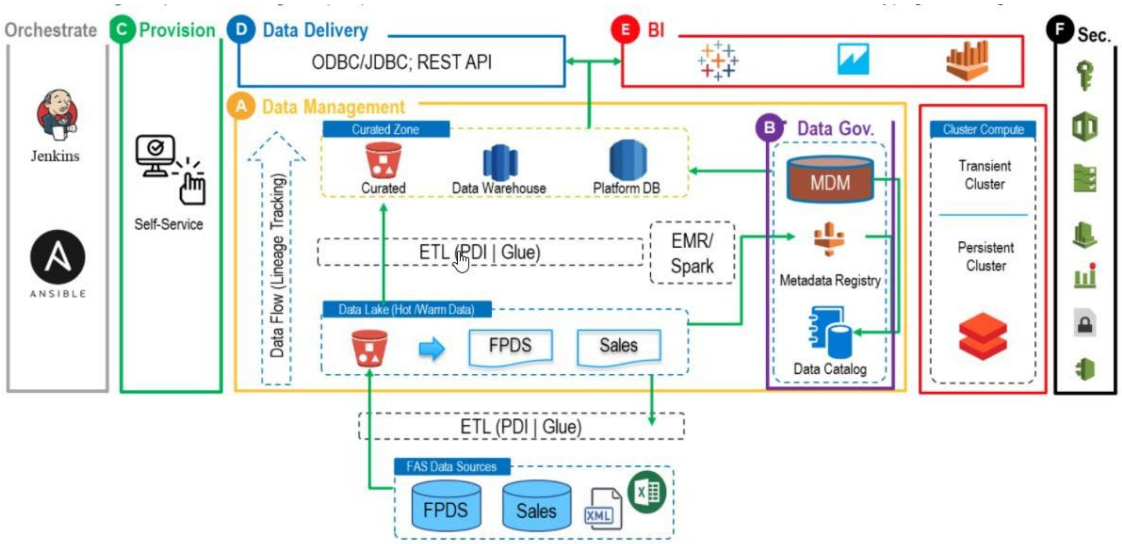


Figure: FAS Data Architecture Logical View

FCS-D Services - Figure 4.9

FCS-D capabilities have two major types of labor support:

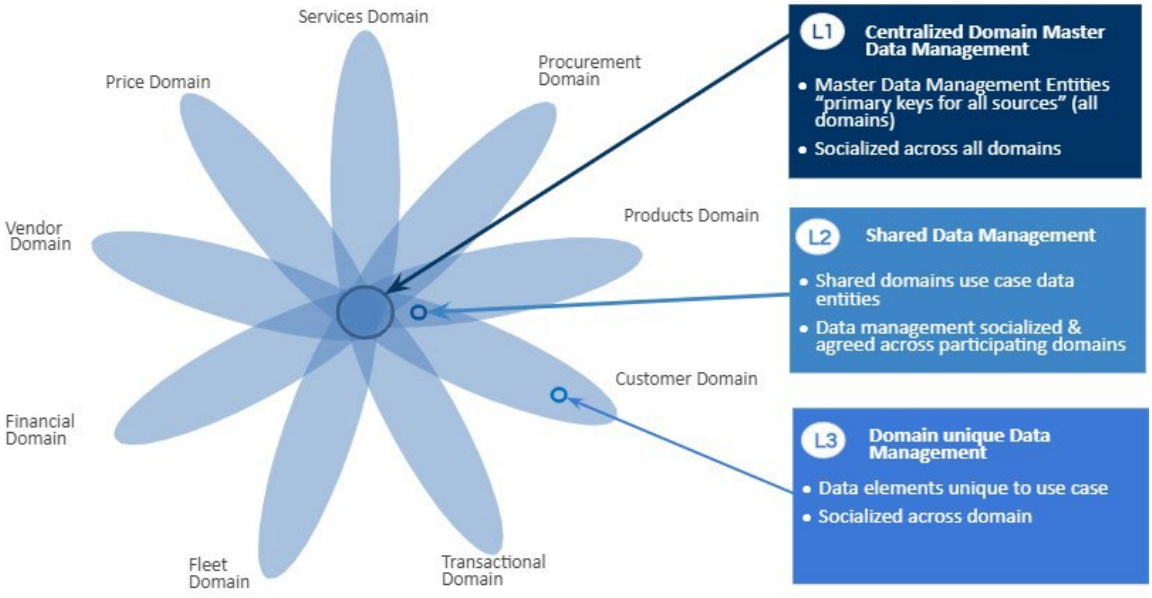
1. Product engineering labor to provide the technology for the tenants and ensure these align with the service agreements in Appendix A - Attachment H - Performance Measures. The set of collective technologies to provide specific capabilities generally referred to as “service”. There are three services in production with two that have been identified for future development and

2. Professional Services to use those capabilities/services for a tenant. The Professional Services are supporting over 65 ETLs for maintaining 38 data sets and collections of corporate reporting as well as visual dashboards forseveral tenants.

All work adheres to the vision from GSA’s Chief Data Officer (CDO) and FAS Data Evidence and Governance Board (DEGB).

1.3.6 Enterprise Data Architecture (EDA)

One major business initiative for FAS is Enterprise Data Architecture (EDA), the goal of this initiative is establishment of a centralized authoritative data on past procurement and operational & performance trends to enable advanced acquisition planning and accelerate insights around demand and supply management. The business defines “domains” as how the business should present data for their community. This is a major step moving away from system data set identification to activity focused. This has resulted in a consistent process for sourcing, modeling, and providing a “single view of data”.



Enterprise Data Architecture (EDA) Domain - Figure 4.10

1.3.7 DEGB - FAS Data Evidence and Governance Board (DEGB)

The DEGB developed the Enterprise Data Architecture (EDA) and was created by the business on how the data is organized. This group of experts established a business managed governance program to mature how this data is structured. GSA IT provides a supporting role to ensure FCS-D is changing services and working with other policy organizations to support DEGB efforts. FCS-D provides the ecosystem for the organization to manage, govern and utilize this data.

1.3.8 VPC as a Service (VPCaaS)

VPCaaS (VPC as a Service) provides tenants the ability to self-provision infrastructure and modernize legacy applications with maximum IT solution flexibility and minimal external dependencies. It provides FCS Tenants with a secure AWS cloud environment with a VPC connected to the FSC's network infrastructure.

This service makes use of FCS's network foundation, which grants tenants the ability to consume FCS services while maintaining independent control of their environment. The network framework grants tenants access to the GSA network for any On-Premise integrations required but doesn't allow direct access to other tenant VPCs. Tenants are responsible for security within their VPC boundary. Since tenants have full AWS access, including access to create Internet Gateways, Peering Connections, and other VPN connections, they are expected to follow all AWS acceptable use policies, and adhere to all FCS and GSA security policies and guardrails.

1.4 Background

On September 13, 2020, the General Services Administration Chief Information Officer established the Office of Acquisition IT Services within it is the Center for Acquisition Systems. Within the Center for Acquisition Systems there are two divisions. The Cloud Integration Shared Services (CISS) Division which handles existing and future GSA IT cloud and integration technology functions, and the FAS IT Modernization Platforms Service Division was established to support the development and execution of the FAS IT modernization strategy and manage the FAS Cloud Services (FCS)EcoSystem, which is built utilizing a published set of standards, patterns, and plays outlined within the FAS IT Playbook[1].

The Office of Acquisition IT Services (FAS IT) provides information technology (IT) support for FAS and other parts of GSA. The applications developed and maintained by FAS IT are used by business portfolios within GSA, customer agencies, the vendor community, and the general public. For each and every business line, the applications supported by FAS IT are essential to daily operations, future growth, and meeting organizational goals.

FAS leverages the buying power of the Federal Government to acquire the best value for both the taxpayers and Federal customers. FAS is organized as follows:

- Management and Program Support
- Office of the Commissioner

[1] http://fas.itplaybook.gsa.gov/

- Office of Customer & Stakeholder Engagement
- Office of Enterprise Strategy Management
- Office of Policy and Compliance
- Office of Systems Management
  - Categories
- Office of General Supplies & Services Categories
- Office of Information Technology Category
- Office of Professional Services & Human Capital Categories
- Office of Travel, Transportation, & Logistics Categories
  - Services
- Office of Assisted Acquisition Services
- Technology Transformation Services

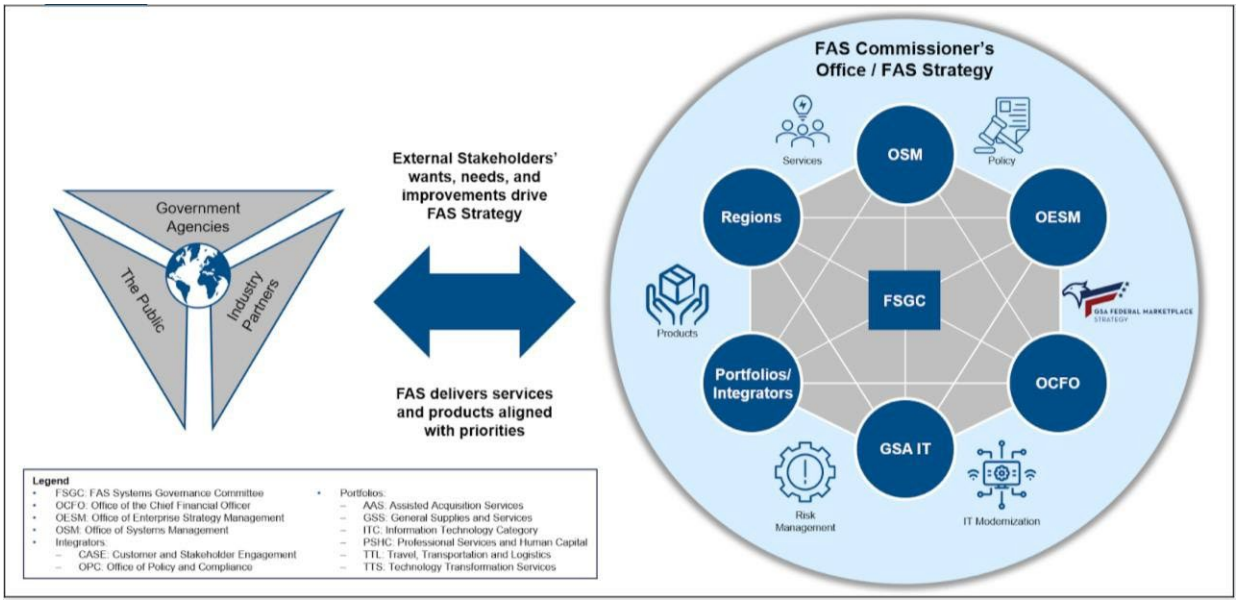
FAS organizations and their stakeholders are the primary users and program offices for the application portfolios that require support under this task order.

The Office of Acquisition IT Services (FAS IT), within GSA CIO, is organized as follows:

  - FAS Managed Services' Systems
- Integrated Award Environment
- Travel and Transportation and Personal Property
- Fleet Management
  - FAS Acquisition Systems
- eCommerce Systems
- Market Research and Digital Experience Services
- Assisted Acquisition Systems
- FAS IT Modernization Platform Services
- Contracts and Supply Chain Systems
- Cloud Integration Shared Services

1.5 Concept of Operations

Over the history of the Federal Acquisition Service (FAS), product and service offerings, along with their supporting systems and technology, were largely developed in silos which aligned to the organizational offices that sponsored them. Communication and partnership across FAS occurred; however, execution continued to largely occur independently, with support organizations, such as the Office of Systems Management (OSM), GSA IT, Office of Enterprise Strategy Management (OESM), and the Office of the Chief Financial Officer (OCFO), acting in an advisory role.



FAS Systems Governance Committee - Figure 4.1

FAS has transformed into a cohesive team of partners with structured coordination by the FAS Systems Governance Committee (FSGC). The FSGC provides an enterprise-wide view across FAS to address existing challenges and future state solutions while simultaneously supporting FAS's ability to operate in solidarity. All partners collaborate, engage, consult, and support each other to enable shared strategic goals and objectives. This organizational collaboration facilitates the transformation of FAS product and service offerings, along with their supporting systems and technology, into agile and modernized solutions that rapidly adapt to the evolving needs of the FAS customer.

One of the ways that GSA IT supports these shared strategic goals and objectives is through the establishment of the FAS Cloud Services (FCS) EcoSystem. The cloud program plays a key role in structuring the people, processes, and technology partnerships within GSA IT to effectively realize the GSA IT cloud strategy through effective FAS IT Playbooks, reusable concept designs and engineering patterns, collaborative strategy planning as well as adoption and operations support for available cloud products and services.

The Vision… GSA IT is rooted in building premier cloud products through collaboration with, and in support of, IT Application teams' priorities and mission to deliver business objectives in the most effective and efficient way possible to take advantage of more efficient processes and technologies that will deliver consistent business value that scales for the agency needs.

The Purpose… the Program is only successful when our tenants and their businesses are successful! Therefore, the Program's purpose is to deliver on the vision for tenants. The Program will accomplish this by providing routine and relevant updates regarding the status of the roadmap, continually evolving the Program's service offerings in responseto tenant demands and maintaining a commitment to value-driven customer service.

1.5.1 Key Objectives:

- Program Enablement

Oversee a product mindset building on an EcoSystem approach to cloud that provides overwhelming customer value and satisfaction for current tenant systems while leading the innovation and transformation strategy supporting the EcoSystem vision.

- Cloud Advisory

Oversee the GSA IT wide cloud intake and strategy development effort that coordinates, advises, and enables GSA IT wide cloud initiatives and investments through established partnerships and processes resulting in collaboratively developed cloud transformation efforts. This utilizes and builds on a set of cloud standards that foster reuse, interoperability and service sharing among various systems.

- Cloud Enablement

Trusted advisory for the adoption of cloud standards and automation that deliver more repeatable and reusable cloud shared services to reduce overall engineering, operations and support schedules and costs. This includes standardizing a way to report cloud economics that provide greater insight into cloud related spend, avoidance / savings opportunities delivering the greatest value to GSA IT

- Innovative and Force Multiplication Cloud Services

Lead delivery of a sophisticated suite of services for the tenant, allowing for increased focus on application functionality resulting in fast time-to-value with lowest stack LOE via ready-to-run stack, automation, templates, and continuous feature additions & enhancements.

1.5.2 Key Goals:

- Centralize Cloud Acquisition Strategy

Increase knowledge-based decision-making with standardized cloud strategy development by providing a GSA IT wide cloud intake and strategy development framework that coordinates, advises, and enables GSA IT wide stakeholders with cloud initiatives and investments.

- Accelerate Value-driven Cloud Adoption

Decrease operational costs with reduced time-to-value by developing cloud services, standards and automation delivering more repeatable and reusable cloud shared services to reduce overall engineering, operations and support schedules and costs.

- Implement Reusable Cloud Services

Consolidate buying power with improved operational efficiencies by providing a standardized way to report cloud economics that provide greater insight into cloud related spend, avoidance/ savings opportunities and investment opportunities delivering the greatest value to GSA IT.

1.5.3 Guiding Principles:

- **Enable Tenant Success**: We continuously strive for tenant success through self-service cloud enablement and provide professional services when needed.
- **Cultivate an EcoSystem of Shared Services**: We provision access to templates and integration patterns for tenants to leverage common,

foundational services and achieve cost, production, and risk mitigation benefits from economy of scale.

- **Apply a Product Mindset**: We orient our organization around products and enabling services, rather than silos of technology.
- **Learn and Innovate Continuously:** We continuously engage with our tenants and evolve existing and add new offerings in alignment with their needs.
- **Deliver Operational Excellence**: We provide reliable, predictable, and consistent products and services through rigorous platform administration, operations, and security so our tenants can focus on their applications and business.
- **Strive for Sustainability and Quality**: We continually evaluate and strive for the right balance between cost, service level, and quality of our offerings.
- **Embed Security in Everything We Do**: We fuse cybersecurity with IT operations, integrating it with infrastructure, applications, and governance.

1.5.4 FAS IT Playbook

The IT Playbook provides guidance on each application's modernization strategy and how the organization intends to leverage ~~a~~ specific design patterns and cloud services as part of the EcoSystem. This foundation establishes consistency that ensures the standardized ~~consistent~~ use of technology and provides more effective interoperability for all development and integration. Through documentedstrategies and published Cloud Plays it standardizes how FAS IT provides structure to the systems that we are entrusted with in the form of sound design patterns, standard practices, re-use frameworks, and a tried-and-true set of common capabilities. This living resource serves our customers as they realize efficiencies through adoption ofstreamlined guidance, purpose-driven templates, compliance to policies, and a solid understanding of business and IT alignment across FAS.

1.5.5 FAS IT Services & GSA IT Shared Services

Charged with leading the GSA IT wide cloud strategy the CISS Division supports the greater GSA IT in achieving the organization's Cloud goals. To-date nearly all of GSA's IaaS and SaaS CSP consumption leverages AWS, however, CISS is responsible for centralizing and standardizing usage of all IaaS and PaaS CSPsunder a single GSA IT Multi-Cloud Strategy. CISS partners and closely coordinates withFCS, whose purpose is to enable the delivery of software applications using modern development paradigms and show significant added value to Federal Acquisition Services (FAS) and GSA wide. Currently a significant portion of the capabilities underthe Program reside in the Amazon Web Services cloud and are architected to leverage the benefits of cloud technologies. FCS has incorporated DevSecOps into its operations.Although the Program has been established to provide services to all of GSA IT, FCS's main focus is to support the modernization of the FAS portfolio, which encompasses legacy, current, and future IT products, services, and systems— throughout the acquisition and system engineering lifecycle.

FCS is a Cloud EcoSystem that delivers the foundational products and cloud services necessary to support GSA's cloud modernization and data lifecycle, providing application teams a quick, repeatable, and easy way to align with the standard development and

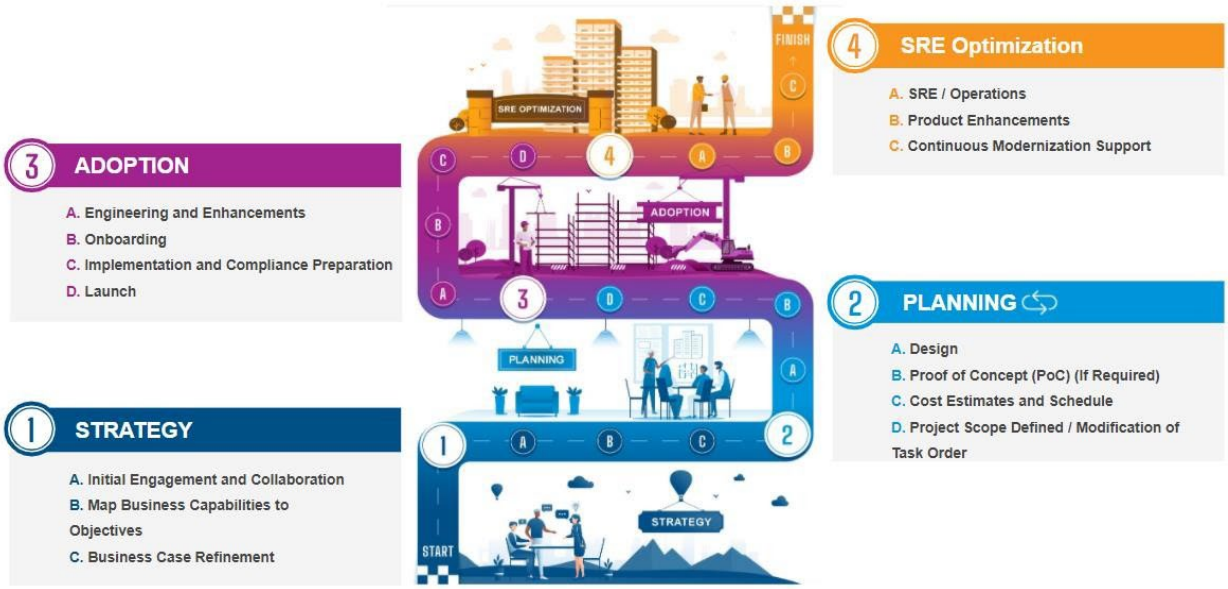
deployment practices established within GSA IT. These services reduce the development overhead an application team has in order to create and manage their business application environment. The results of the services are consistent with industry best practices, deliver reduction of redundant capabilities, expedite needs-driven technical adoption, promote response-driven security, and are a force-multiplier for supported business lines. To ensure necessary reuse and standardization while also not inhibiting valuable innovation, cloud services may be engineered and operate under this task order as either organization level services (FAS) or as Shared Services supporting broader adoption (GSA IT wide). This task order directly accounts for the success of both FAS IT Services (FAS IT funded services) as well as Cloud Integration Shared Services (GSA IT / Working Capital funded services).

Today FAS Cloud Services offers over six fully featured services (three technical and three labor), which are detailed further within the Cloud EcoSystem section of this task order Cloud Program Overview section. These Services enable application teams to expedite feature first development. FCS also has a specific operation focused on supporting the work related to the many aspects of working with data, such as storage, research, evaluations, and dissemination. Over one-third of the addressable market for IT systems have been able to deliver value to their stakeholders by leveraging these cloud and data services. Within Cloud Services - Figure 4.4 you will find the current state of the cloud services landing zones and respective products that are supporting, or anticipated to support, the business systems identified within Cloud Tenant Roadmap - Figure 4.1. Additional information related to this topic can be found within the FAS IT Cloud Enablement Roadmap[2] in the FAS IT Playbook within the link in the footer of this page.

1.5.6 Cloud Advisory and Enablement

Fundamental to FAS IT Modernization - and a significant forward-driver of this - is our Cloud Enablement (CE) Roadmap. We have developed this detailed CE Roadmap (Figure 4.2) as a basis and facilitator of the system-by-system modernizations currently underway. The phases spelled out in the CE Roadmap provide specific milestones and targets upon which the new, re-engineered and modernization applications will land. The CE Roadmap strategically introduces technologies, tools, and techniques over time to accelerate Cloud Adoption enabling business lines to modernize their applications, improve their productivity and improve their end-user satisfaction and adoption.

[2] FAS IT Playbook Enablement Roadmap: https://sites.google.com/a/gsa.gov/fas_it_playbook/it-playbook/fas-cloud-services/transformations



Cloud Enablement (CE) Roadmap - Figure 4.2

Phase 1: Strategy

Establishes a foundational approach to address business requirements with fiscal responsibility. The key to any successful cloud journey is early engagement, collaboration, and a deep shared understanding of the core business objectives amongst an integrated team representing the business, application developers, Cloud Integration Shared Services, FCS, and IT Security.

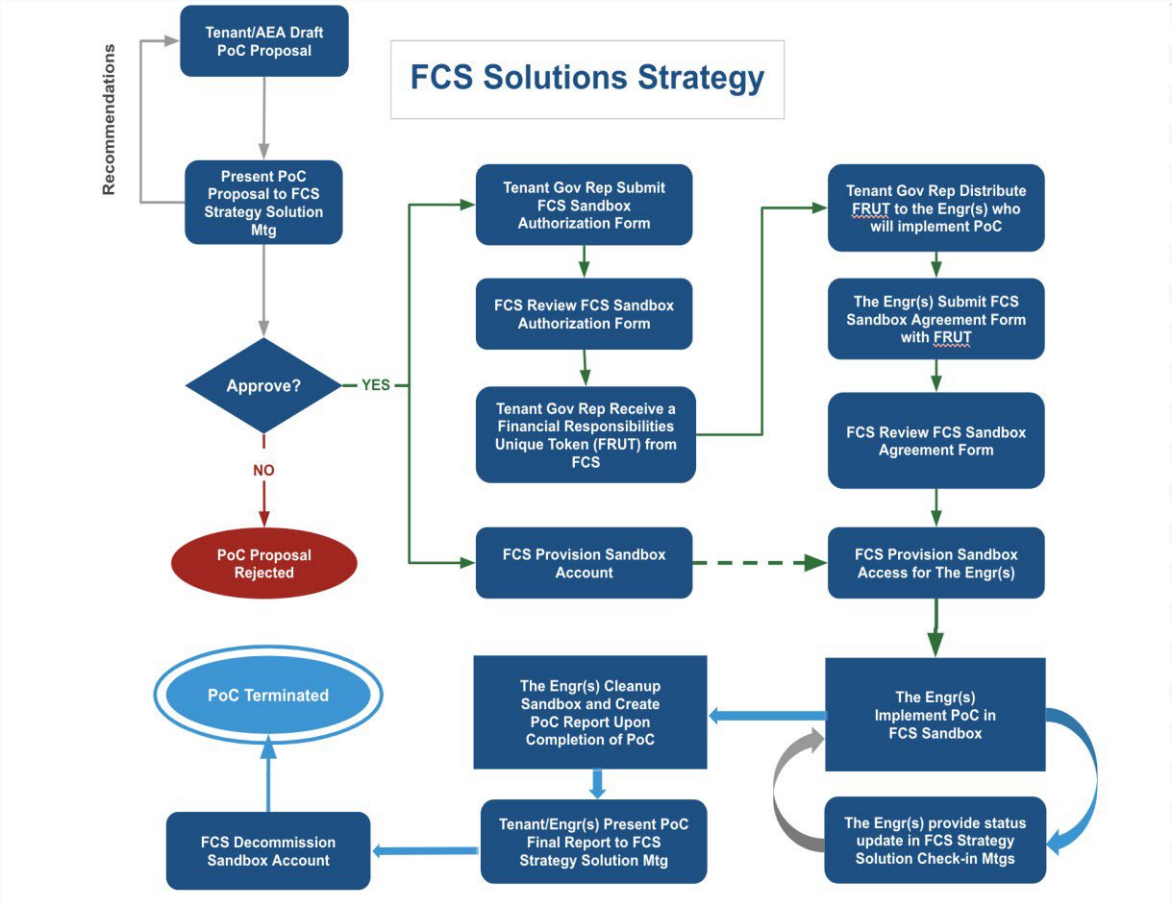
Phase 2a: Planning

This phase begins once the cloud strategy has been agreed upon by all IPT representatives. An extensible Cloud Strategy to facilitate implementation of the intended solution. Throughout the Planning Phase, capabilities are aligned to business requirements. Where gaps are identified, a Proof-of-Concept may be required to validate a proposed technical solution. Potential vendors should be able to understand the requirements and desired solution.

Phase 2b: Proof of Concept

When objectives and requirements are reviewed within the Cloud Enablement process, results may recommend a Proof of Concept (PoC) proposal. This PoC process (Figure 4.3) is how GSA IT encourages innovation, promotes continuous improvement and optimization. The proposal must explain what Technical Capability the PoC is validating or proving as an option for a larger solution as well as clearly defined success criteria. All stakeholders can create a PoC proposal and follow the process below to utilize a sandbox[3] as part of requirements development.

[3] https://sites.google.com/a/gsa.gov/fas_it_playbook/it-playbook/fas-cloud-seívices/offeíings



Process for Proof of Concept - Figure 4.3

Phase 3: Adoption

This phase begins when all Cloud services are available to support the Cloud Strategy. Cloud Solution is ready to launch with Authority to Operate. During the Adoption phase, the Cloud environment is established according to the selected services to support the technical solution. The Development team begins to iterate and deliver the intended solution with support from the Cloud Enablement Team. The product is prepared for the production environment.

Phase 4: Site Reliability Engineering (SRE) Optimization

This phase is when a fully enabled Cloud Solution is deployed with ATO, and then continually optimized. A modernized product is deployed which provides business value to FAS Stakeholders. Site Reliability Engineering (SRE) Optimization begins and the environment is continually optimized, monitored, issues are tracked and enhancements are incrementally delivered.

1.6 Applicable Documents, Definitions, Abbreviations & Acronyms

The documents (i.e., certifications, specifications, standards, policies, and procedures), current at time of contract/order award, identified in the list below, are incorporated with the same force and effect as if provided in full text. Succeeding revisions may be substituted or

incorporated as required with full notice and disclosure to the contractor. The Government will provide access to available documents and technical information as required and upon contractor request, if not available via a hyperlink within this PWS.

1. Applicable Document
See Attachment A, Tabs B, C, F, G, L, M and security documents listed in Section 8, below.

2. Definitions, Abbreviations & Acronyms
See Attachment 1, Tab K

2A ADMINISTRATIVE OBJECTIVES AND REQUIREMENTS

2A.1 General Performance Requirements

2A.1.1 Resources

It is the Government's objective to rely upon Contractor resources to perform this requirement. To meet this object, the Contractor shall furnish or provide all personnel, personnel management and supervision, all related internal supporting business functions (including background and "overhead" personnel), materials, supplies, equipment, and facilities to perform the full range of services required by this PWS. Exceptions shall include government furnished items or data if so stipulated in Section 7, below.

2A.1.2 General Communication

It is the Government's objective that the Contractor maintain regular and direct interface with the Contracting Officer (CO); the Contracting Officer's Representative (COR), and other identified Government representatives. The contractor shall not contact nor take direction from unauthorized Government representatives, under any circumstances.

Government personnel will be made available to provide technical strategy and input, answer questions, review completed draft deliverables, and provide feedback.

2A.1.3 Identification of Employee Affiliation

In compliance with FAR 37.144(c), contractor employees shall avoid creating an impression in the minds of members of the public or Congress that they are Government officials by taking the following measures.

- All contractor personnel shall be required to wear Government-approved or provided picture identification badges so as to distinguish themselves from Government employees when working at the Government site.
- Additionally, the contractor shall comply with all visitor identification requirements when visiting the Government site.
- When conversing with Government personnel during business meetings, over the telephone or via electronic mail, contractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees.
- Contractors shall identify themselves on any attendance sheet or any coordination documents they may review.
- Electronic mail signature blocks shall identify their company affiliation.

- Where practicable, contractors occupying collocated space with the Government should identify their workspace area with their name and company affiliation

2A.1.4 Business Relations

A primary element of project success is the business relationship between the contractor and Government representatives. It is the Government's objective that a successful business relationship be maintained. The Contractor shall contribute to meeting this objective by making every effort to establish and maintain clear and constant communication channels with the Government authorized representatives for the purpose of:

- Promptly identifying PWS and/or business relationship issues of controversy and the bilateral development and implementation of corrective action plans.
- Ensuring the professional and ethical behavior of contractor personnel.
- Maintaining effective and responsive subcontractor management (if applicable).
- Ensuring the contractor support team is fully aware and engaged in strengthening the interdependency that exists between the contractors and their Government counterparts.
- Facilitating contractor–Government collaboration for continuous improvement in performing PWS tasks, reducing risks and costs, and meeting the mission needs.
- Providing meaningful feedback during discussions about project execution, when required.

- Complying with all GSA policies regarding contractor personnel

2A.1.5 Contractor Response

The contractor shall ensure prompt response to Government inquiries, requests for information or requests for contractual actions. Unless otherwise specified in the PWS, a prompt response is considered acknowledgement by the contractor within one business day. The response will either provide the requested information or action, where feasible to complete within that time frame, or propose a timeframe, for mutual agreement, in which the request will be completed.

2A.1.6 Professional Appearance

It is the Government's objective that all personnel involved with this project present a professional appearance. To meet this object the Contractor personnel shall present a neat and professional appearance appropriate to the work being performed at all times when interacting with Government representatives, working in Government facilities, or representing the Government at meetings or before third parties.

2A.1.7 Team Continuity and Employee Retention

The Government recognizes the benefits in maintaining the continuity of contractor team members. These benefits include but are not limited to retention of corporate knowledge, minimizing contractor familiarization, maintaining/increasing performance levels,

schedule adherence and preserving organizational interfaces developed over time. These benefits also accrue to the Contractor. Within the context of effective and efficient personnel management, the Contractor shall take reasonable and appropriate steps to retain the qualified employees staffed against this contract to maintain continuity and performance while effectively reducing costs borne by the Government.

2A.2 General Meeting Requirements

The contractor shall participate in the following meetings. Nothing discussed in any meetings or discussions between the Government and the contractor shall be construed as adding, deleting, or modifying the contractual agreement without written authorization from the Contracting Officer.

2A.2.1 Initial Business/Kickoff Meeting

Within 5 business days following the contract/order award (or other time mutually agreed between the parties), the contractor and its key personnel shall meet with the GSA CO, GSA COR, and other identified Government representatives to ensure a common understanding of the requirements, goals, expectations, end products, and objectives of the contract/order. The contractor shall discuss the overall understanding of the project and review the background information and materials provided by the Government. Discussions will also include the scope of work, deliverables to be produced, how the efforts will be organized and project conducted; assumptions made/expected end results. A concerted effort shall be made to gain a thorough understanding of the Government expectations. However, nothing discussed in this or in any subsequent meetings or discussions between the Government and the contractor shall be construed as adding, deleting, or modifying any contract/order requirements, including deliverable specifications and due dates. The contractor shall also address the status of any issues that will affect contractor start-up/ramp-up toward achieving full service/support capability. The contractor will be responsible for taking minutes of this meeting. This meeting can be held at either the Contractor's or Government's location, as appropriate.

2A.2.2 Monthly Status and Ad hoc Technical / Work Status Meetings

The contractor shall, if requested by the Government, participate in monthly status meetings or ad hoc technical meetings at a mutually agreeable time and place to discuss tasking, work progress, technical problems, performance issues, or other technical matters. During these meetings the contractor shall at least provide accomplishments, problems and issues, and planned actions. The contractor shall take minutes of these meetings and include them in the Monthly Status Report. These meetings will occur at a time and place mutually agreed upon by the parties.

The Contractor shall maintain project milestones for each assigned task. The Contractor shall update Government representatives on work progress and task milestones during the monthly status meetings.

2A.2.3 Contract Administration Meetings

The CO may require the authorized contractor representative to meet or participate in a teleconference with authorized Government personnel as often as deemed necessary to discuss performance or administrative issues. The contractor may also request a meeting

with the CO when deemed necessary. The content of meetings shall be documented in writing, as agreed between the parties. Minutes shall be approved by both parties and shall be included in the Government contract file.

2A.3 Program / Project Management Requirements

2A.3.1 General Program / Project Management Requirements

The contractor shall be solely responsible for managing the work performed in the execution of the contract/order. This includes the responsibility to:

- Assign appropriate resources to each task.
- Maintain clear organizational lines of authority.
- Ensure effective task management and administration, following the requirements set forth in the PWS.
- Maintain the personnel, organization, and administrative control necessary to ensure that the work delivered meets the specification requirements.
- Establish and use proven policies, processes, analyses, and best practices.
- The contractor shall be fully responsible for management, control, and performance of any subcontractor used in support of the contract/order. Use of a subcontractor on the contractor's team shall not relieve the prime contractor of responsibility nor accountability in the execution of the contract/order

Additionally, the contractor shall:

- Bring problems or potential problems affecting performance to the attention of the CO as soon as possible.
- Notify the COR, CO, and other identified Government representatives immediately of any projected, anticipated, or known delays that may impede contactor performance.
- When requested, deliver written reports to the CO to memorialize all verbal reports.
- Provide, in writing, the results of all meetings in which proposals are put forth that have the potential for affecting and/or changing contract agreements, requirements or conditions, and these shall be brought to the attention of the CO.

2A.3.2 Phase-In Support

The contractor shall provide phase-in support in accordance with the phase-in plan as required per PWS paragraph 4.5.9

2A.3.3 Phase-Out Support

The contractor shall provide phase-out support in accordance with the phase-out plan as required per PWS paragraph 4.5.10

2A.4 Subcontract Management

The Contractor shall be fully responsible for management, control, and performance of any Subcontractor used on this contract. If a Subcontractor is being used, the Prime Contractor

must inform the Government. Use of a Subcontractor on the Contractor's team shall not relieve the Prime Contractor of responsibility nor accountability in the execution of this contract/order.

The contractor shall apprise the government before a new subcontractor, at any tier, is added to the prime contractor's team and shall provide a brief explanation of the benefit of the addition.

2B Technical Objectives

2B.1 Objective 1: Program Enablement

While the government recognizes that Program leadership and oversight is a core consideration driving the success of the program, we are not seeking a traditional top down PMO approach to support the Cloud Program. Based on a product modeled organizational structure, the program enablement work should achieve a balance of leadership, vision, and value alignment partnered with operational cohesiveness, standards development, product maturity, and excellent support. It is crucial that both the product teams as well as those leading them maintain a collective balance of short-term goals matched with longer-term objectives. The government envisions Program Enablement as fostering technical leadership and providing the tools and process necessary to link tenant needs with the services and support that we provide. Program enablement sets Objectives and Key Results(OKR's) (FY22 Program OKR's provided within Appendix A, tab E) based on feedback fromtechnical and program leadership and ensures that the resources and tools are available toensure success with the implementation of the objectives. An example would be proactive support and advisory considerations for program adjustments to new requirements and initiatives related to the recently published *Executive Order on Improving the Nation's Cybersecurity, (Section 8.2).*

2B 1.1Sub-objective: Program Leadership

With a view on delivering value through measured growth, the Cloud Program continues to invest in a management approach that establishes and implements project and product management best practices for the benefit of future goals, in a way that encourages collaboration, standardization, and overall improvement in meeting Objectives, via Key Results, across the organizational landscape. Industries that achieve best-in-class products and services through transformation adhere to program management through a lens of product mindset, agility, collaboration, and transparency, and not as overhead or oversight. Core program management activities such as staffing, schedule, risk management, budget, and financial reporting are critical in support of modernization. This approach is one that an offeror should exhibit and detail, to successfully accomplish task order requirements, build the right product(s), minimize performance and cost risk for GSA.

2B 1.1.1 Program Financial Management

This program requires tracking of expenses for several different audiences. The Cloud Services program classifies users of the services as Tenants. These tenants require a monthly invoice detailing the costs of the services, professional services or

consumption.

Program Execution

There is no substitute for effective program management and project execution. The contractor shall implement and follow a program management approach that:

- Ensures Disciplined Execution
    - Set and understand clear goals, objectives, scope, and outcomes
    - Manage cost, schedule, and performance to deliver on commitments.
    - Proactively identify and manage risks before they lead to unforeseen impacts
    - Establish a Definition of Done (DoD) framework for all work to be performed
- Understands and Delivers Value in the Eyes of the Customer
    - Code and system enhancements are of no value to GSA and its customers until they are running in production, apply Definitions of Done
    - Technology and development must have a clear business or mission driver
- Provides Constant Visibility and Transparency
    - Transparency promotes better performance and accountability across teams and team members.
    - Enhance communications correspondence to tenants via CISS Newsletter containing news and other topics of interest.
- Is Agile and Delivers Value Iteratively
    - Design, build, and iterate on minimally viable products (MVPs)
    - Implement lean processes and minimize Work in Progress (WIP) and consistently deliver to production
    - Prioritize tasks which deliver the highest value for the enterprise and reduce operating costs with the shortest duration of work
- Ensures Consistently Credible, Accurate Cost Estimates
    - Provide a consistent methodology, approach, and techniques to estimate resources, time, and cost requirements & templates in planning and discovery
- Recommend improvements and enhancements to FCS business, service, infrastructure, processes, and support service to better improve the business functionality and customer experience.
- Achieve, maintain, and report compliance with policies and guides published by GSA IT.
- Create and utilize a document management structure within Google Drive that will centralize documentation increasing internal and external awareness to published reference material including version and publication control procedures.

2B 1.1.2 Program Management Plan

The contractor shall provide the Government with a draft Program Management Plan

(PMP), on which the Government will make comments. The final PMP shall incorporate the Government's comments. The PMP will be updated as changes in the program occur. The document will be reviewed and updated as needed on an annual basis, at a minimum. The contractor shall conform to the latest Government approved version of the PMP.

The contractor shall develop a PMP including but not limited to the following:

- Describe the proposed management approach
- Contain detailed Standard Operating Procedures (SOPs) for all tasks
- Include milestones, tasks, and subtasks required in this TO
- Provide for an overall Staffing Strategy to include, but not limited, roles and responsibilities
- Maintain a Stakeholder Management Plan and associated partnerships between or among Government organizations and other COMET contractor teams
- Create and maintain an Incident Response Plan
- Create and maintain a Configuration management Plan
- Create and maintain a Risk Management Plan

2B 1.1.3 Program Performance Measurements

Products and Services delivered and maintained under this contract shall meet the defined service level objectives (SLO's) and/or performance measures outlined within Attachment 1, Tab H - Performance Measures and maintained within the Quality Control Plan (QCP). To effectively ensure the anticipated level of reliability it will be anticipated that it will be necessary to operate Cloud Services product and services teams utilizing a Service Reliability Engineering (SRE) model that sets, monitors, and achieves Performance Measures while reducing time spent on manual or toil tasks.

The contractor shall coordinate and align reliability actions and activities within the product team velocity. Coordinate incident response to services between SRE members for each product and services team in a way that expedites partial and/or full outages to minimize tenant downtime to the greatest extent possible. Ensure that through proper SRE planning and prioritization each product team is appropriately accounting for all support, patching, maintenance, and other typical operational activities as part of defined program increment and sprint planned velocity.

2B 1.1.4 Performance Measures

The government has listed current performance measures in Attachment A, Tab H. Beneath the current performance measures the Offeror can propose measures they deem relevant and of benefit to the Government. Post award, the contractor shall partner with the government to build out the Offeror proposed performance measures.

2B 1.1.5 Quality Control Plan

The contractor shall provide the Government with a draft Quality Control Plan (QCP), on which the Government will make comments. The final QCP shall incorporate the

Government's comments. The QCP will be updated as changes in the Program occur. The document will be reviewed and updated as needed on an annual basis, at a minimum. The contractor shall conform to the latest Government approved version of the QCP.

Cloud Performance Measures are found in Attachment 1, Tab H - Performance Measures.

The contractor shall be responsible for reporting Quality Assurance monitoring for all products and services under this contract's QCP to the Quality Control Assessment Monitoring Office and designated Quality Control Representatives. The contractor reported levels of service and quality assurance provides monitoring for key services provided in this Task Order's Service Level Objectives and Performance Measures. All Quality monitoring pertaining to Service Level Objectives and/or Service Level Agreement items shall be reported and managed as outlined in the overarching BPA Quality Assurance Plan and Quality Assurance Monitoring sections of the contract/task.

2B 1.1.6 Program Status Report

The contractor PM shall develop and provide a Monthly Status Report (MSR) to the Technical Point of Contact (TPOC) and the Contract Officer Representative (COR). The MSR shall at a minimum include:

- Activities during the reporting period, by application, which include any on-going activities, newly started activities, activities completed and activities planned (30/60 day outlook); progress to date on all above-mentioned activities; and cost and schedule performance.
- Summarize the impacts of any new software released, and the business value of the releases to GSA and/or the Government as a whole.
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- Personnel gains, losses, vacancies (including durations of open billets), and status (security clearance, etc.).
- Training provided to current staff.
- Government actions required.
- Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for the reporting period).
- Accumulated invoiced cost for each CLIN through the previous month, reported by Application.
- Projected costs of each CLIN for the current month, reported by Application
- Estimated costs at completion of the current period of performance reported by Application (Base or Option Period).
- Significant High and Critical Program Risks Summary.
- Summary of Security Vulnerabilities and Trends by Application.

The contractor shall convene a Monthly Status Meeting with the TPOC, COR, and

other vital Government stakeholders. The purpose of this meeting will be to present the MSR in order to ensure all stakeholders are informed of the monthly activities and provide opportunities to identify other activities and establish priorities, manage costs, and coordinate resolution of identified problems or opportunities.

The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned to the TPOC and COR within two workdays following the meeting.

2B 1.2 Sub-objective: Technical Leadership

Bring emerging approaches, technologies, capabilities, and new partners to increase the value that is provided to FCS cloud customers. As FCS continues to evolve the platform offerings (current/ proposed) and management services, it must align technical decision making to a single architectural vision and strategy. Achieving a common vision will allow the program to maximize energy applied towards reducing technical debt, promoting best practices, consolidating duplicative offerings, and expanding the platform capabilities for tenants. Additionally, as part of AWS infrastructure analysis, achieve optimization of cost through transparency and reporting, identification and implementation of solutions that reduce cost of infrastructure, tools, licenses, etc., and improvement efforts that streamline operations and scale delivery of FCS offerings.

To meet this objective, the contractor shall perform the following:

- Provide strategic insight into the service areas and identify architectural and operational optimization opportunities based on current FCS service offering
- Contribute to and lead as necessary laying out the roadmap for overall FCS and CISS cloud architecture evolution and each product and shared service, aligning with GSA IT vision
- Develop architecture maturity measurement framework for tenant's portfolio and applications
- Develop a cloud economist model and cost control strategy
- Design and execute GSA IT mission-driven proof of concept
- Lead initiatives and contribute to Cloud Advisory and Enablement documentation
- Perform analysis of alternatives (AoA) for emerging technologies, develop analysis reports and presentations and support decision making process of technology, service, tooling selections

2B 1.3 Sub-objective: Operations Leadership

It is imperative that the cloud program maintain the cloud products and services operational stability, quality of service, compliance with GSA Security guidelines, and capacity for implementation of rapidly changing needs is fundamental to technical operations in accordance with performance measures outlined within Attachment 1, Tab H - Performance Measures. Execute on the Incident Response Plan and Configuration Management Plan to manage incidents, problems, and changes. Coordinate configuration changes and updates related to product changes or enhancements, as necessary, with Product Owners and follow the Cloud Enablement process to evaluate

any solutioning.

2B 1.3.1 Cloud Services Support

Fundamental to GSA IT is to deliver desired business outcomes and success. In other words, value in the eyes of the customer. To accomplish this the contractor must not only view success as delivering value through features but also managing and maintaining the system in a consistent and ever improving fashion to modern DevOps practices. The Government would consider any proposed recommendations that would optimize Cloud Service Support through an effective staffing strategy and result in quicker resolution to issues occurring during off hours.

To meet this objective, the contractor, within the operations framework, shall account for, at a minimum, the following activities below:

- Achieve all support related performance measures as maintained within the QCP
- Provide problem resolution support, identify and resolve problems, fix defects in the technical system architecture and configuration, coordinate with system users to determine symptoms and ensure accurate problem definition and resolution within SLO
- Leverage ChatOps to effectively communicate and collaborate between internal team, tenants, and the government
- Continuously update and adapt to a modern DevOps practice. This includes already standardized frameworks within GSA such as Site Reliability Engineering (SRE)
- Continuous improvement activities throughout the support process
- DevOps team toil tasks (don't separate 'engineering' vs 'ops') All DevOps / SRE staff must understand how the system is being used and the challenges experienced by users
- Monitor toil tasks performed and reduction measures taken to meet/ exceed SLO
- Deliver business capabilities that can be readily supported and maintained, by different teams if necessary, through the life of the system
- Provide Level 1/Level 2 (L1/L2) support (further outlined within Cloud Enablement Triage Team (CETT))
- Utilize an automated ticketing processes for support desk management
- Conduct Root Cause Analysis (RCA) requesting support from Product Owner/Technical Lead as needed on critical incidents and track completion of any identified preventative action items to reduce incident recurrence.
- Identify and assess any patterns of occurring incidents or service degradation in the environment and engage Product Owner/Technical Leads to develop strategy to address and submit to GSA Leadership for consideration.
- Coordinate and maintain Service Level Objectives (SLO's) with tenants, to include routine maintenance, unplanned outages, out of cycle maintenance, major and minor component upgrades, and incident response targets.

- Establish and maintain SLOs with FCS leadership, to include response time for Level 1 and Level 2 support tickets.
- Coordinate operations activities (e.g., patching, security remediation, version upgrades, etc.).
- Work with the government leadership to define the scope and implement a sustainable Off Business Hours support model, which outlines the process for submitting and approving an Off Business Hours support request, based on criteria requirements.
- Review existing operational processes, present any identified gaps and areas for improvement to GSA leadership for consideration.

2B 1.3.2 Customer Service Management

FCS utilizes Customer Service Management software for managing and tracking generic requests and reporting service incidents. In addition, FCS uses Google Hangouts chat rooms to provide FCS Chat Operations for real time support and collaboration with customers and team members.

The contractor shall be responsible for:

- Entering, tracking, updating, and closing support cases utilizing the Customer Support Management software in real or near real time as they occur. (Including chat communications)
- Update communications, escalations, identified issues, fixes, configurations documenting any update or change to the status of the Customer Support cases.
- Managing access to Customer Service management software interface for staff and customers to engage FCS Cloud services and support.
- Maintain inventory of available FAS Cloud Services including associated tenants leveraging each of the services.
- Manage the process and identify new enhancements to that software that improve support and services to the FCS business and its customers.
- Track and report performance measures for tickets logged to FCS based off SLO’s
- Keep the FCS Portal updated with the latest information.
- Provide ease of use tenant SOP to request, access, and utilize FCS
- Establish a process to manage a funnel of commitments and create a reporting method to prioritize and communicate new engineering requests submitted by tenants.

Attachment 1, Tab L - Standard Operating Procedures contains the list of FCS Standard Operating Procedures (SOP) utilized on a regular basis to ensure stable and repeatable operations. This does not represent all SOP’s supporting FCS but has been provided to help represent areas of recurring support.

Cloud Enablement Triage Team (CETT)
The Cloud Enablement Triage Team (CETT) manages operations using a ConOps

model which includes Cloud Foundations made up of common components and support that provide the basic fundamentals for operating and supporting GSA systems within the FCS EcoSystem. These foundations include, but are not limited to, network, identity management, patching for shared capabilities, security/ATO for shared capabilities, and tenant experience support.

Built on the Cloud Foundations, the Program has defined Services and organized them into Product Lines. Each Product Line is made up of a set of products with defined features. Additional features and/or products are introduced as needed to increase business value and/or as products reach end of life. The Product Lines provide tenants the flexibility to leverage cloud at various levels of application cloud-readiness and provide a path for maturing to more automated and managed services and more inherited security controls.

Initial Response Support: This Level 1 (L1) support is the initial interface with Cloud Services and triaging all incoming support requests through the ticket management process in accordance with the SLO performance metric. The contractor shall be responsible for:

- Staff technical engineering skills and services support expertise to independently troubleshoot and resolve level 1 issues.
- Monitor patterns in tenant requests to work with Cloud Services Support / product owners.
- Manage the Cloud Enablement process to evaluate if cloud strategy or services need to be created or altered to include the program's ChatOps process, which is the primary method all tenants are encouraged to troubleshoot service issues.

Core Tenant Support: This Level 2 (L2) provides engineering support to guide the tenant experience. Collaborate between tenant and engineering/SME support to enable customer success. The contractor shall be responsible for:

- Develop/maintain report metrics, manage service requests & incidents triaging, providing L1 and escalation support in accordance with the SLO performance metric in the Cloud Service Appendix, Attachment 1, Tab H - Performance Measures.
- Provide intake of tenant requests, collaborating on priorities and tasks. Complete FCS account requests, coordinating tenant access to systems.
- Provide direct support, as requested in advance for deployments and other tasks.
- Recognize trends in support requests and work with product owners to define features and/or process improvements that will improve the tenant experience and promote self-help.

Technical / Adoption Support: This L2 support requires the engineers who are the experts in the products/services for resolving issues from the ticket management process in accordance with the SLO performance metric. The contractor shall be responsible for:

- Staff technical engineering skills and services support expertise to independently troubleshoot and resolve L1 and L2 issues.
- Monitor patterns in tenant requests to work with Cloud Services Support / product owners.
- Manage the Cloud Enablement process to evaluate if cloud strategy or services need to be created or altered to include the program's ChatOps process, which is the primary method all tenants are encouraged to troubleshoot service issues.

Understanding and correctly addressing the greatest support impacts results in more reliable cloud systems. Below are the top 5 support considerations representing January 1st 2020 to May 1st 2021.

1) **There have been 4844 tickets** (Includes both incidents and requests)
   - L1: 1499 (30.9%)
   - L2: 1497 (30.9%)
   - IDM: 1812 (37.4%)
   - Security: 36 (0.7%)
2) **The percent of issues resolved at L1 vs escalated to L2 is 49.4%** (Excludes IDM/Security)

3) **Top 5 most common support topics make up 27.6% of the tickets**
   - **Jenkins (123 tickets - 8.2%)** - Understanding of Jenkins and services that Jenkins interfaces with (i.e. Artifactory, AWS services, GitHub, and Splunk)
   - **Artifactory (96 tickets - 6.4%)** - Understanding of Artifactory including both its user interface and the process of uploading packages from package managers like maven and npm.
   - **RDS (81 tickets - 5.4%)** - Understanding of RDS including high level concepts about supported databases, the RDS AWS console, and how RDS can be configured.
   - **DNS (65 tickets - 4.3%)** - Understanding of, and access to, NetScaler as well as an understanding of DNS.
   - **Marketplace for CaaS (50 tickets - 3.3%)** - Understanding of the custom Marketplace application, developed for CaaS, including its interface, supported functionalities, and development/testing processes.

The balance of the topics fall into other related activity areas.

The government believes that enhanced support can be accomplished through the establishment of a user / developer community. This community will establish collaboration and enable support, contribution and participation from a broader stakeholder group than just this contact. Support provided and domain knowledge captured through this community should be available to all tenants and easily searchable to enable teams with questions or issues to utilize research and problem-solving skills to help resolve operational and adoption issues, where possible, without the help of FCS team members.

To meet this objective, the contractor shall perform the following:

- Automate a tenant facing support portal that provides transparency, promotes collaboration, and publishes searchable issue/resolution information.
- Regularly reviews and enhances the design principles and best practices in modern software development and deployment that leverage cloud technologies. This consists of stakeholder collaboration and necessary tooling to empower applications teams to efficiently deploy their applications following the standard GSA IT process.
- Establish a cloud enablement support team to perform the following.
    - Main point-of-contact for tenants to work with FAS Cloud Services and provide knowledge and expertise on how tenants can adopt the services as developed for support from FAS Cloud Services.
    - Provide Service Delivery Management to organize and ensure requests/requirements from the tenants are triaged and classified to the Cloud Enablement process.
        - Routine meeting to review the high-level objective and risks for each tenant
        - Evaluate how each tenant is progressing on their approved cloud strategy
        - Communicate recommendations that will likely help the Application teams experience with FCS capabilities based on current or future services.
- Maintain the authoritative repository of FCS processes, procedures, and other materials necessary to deliver and support cloud services for GSA IT applications in a consistent and repeatable fashion.

2B 1.3.3 Change Control Board (CCB)

A key consideration for change control is to establish and operate the Change Control Board (CCB) to review and approve changes and requests affecting all environments necessary to control costs, control scope changes, and provide historical data for quality assurance purposes for technical changes, software development, projects and programs. The CCB committee will consist of Subject Matter Experts (SMEs) and PMs/POs who decide whether to implement proposed changes into the cloud environments.

To meet this objective, the contractor shall perform the following:

- Manage and maintain the processes and procedures necessary to evaluate operational change requests weekly for potential business, operational, policy, and security impacts.
- As necessary, issue new change control processes to adapt to the continuously expanding scope of products and services.
- Create and/or maintain tools and processes to capture and track all changes and associated details and supporting documentation.

- Ensure adequate description, impact(s), implementation steps, backout steps, and justification of each change is captured to describe the change and its impacts to the baseline of the product and any other dependency as a result of the change.
- Manage and facilitate weekly CCB with GSA Stakeholders/Product Owners/Technical Leads to coordinate and obtain necessary approvals for submitted changes.
- Support the change by providing the necessary artifacts according to the type of change (major, minor, patch, hotfix, etc.).
- Maintain the types and level of artifacts required for each change type as prescribed in a Configuration Management (CM) Plan.
- Validate all test results completed under the Change Management Testing requirements or if automation is not possible it has to be justified within the change request
- When applicable, require that submitted changes have a test plan and evidence of the test results prior to approval.
- Ensure that changes submitted by other GSA organizations (network, security, etc.) are adequately documented and described. Coordinate these changes within the program delivery cycle.
- Require that all changes to the Cloud Services environment are well communicated and coordinated with the tenant base.
- Review and approve operational change requests (version upgrades, bug fixes, etc.) to the Cloud Services environment prior to changes being made to a production environment, which will result in reduced risk to unanticipated outages for products and services as well as tenant application environments.

2B 1.3.4 Technical Evaluation Process (TEP)

To properly control and assess technical changes and enhancements to the cloud environment, the Cloud Services has implemented a Technical Evaluation Process (TEP) which is an enforcement gate for the necessary information to evaluate for possible impact prior to production deployment. TEP gives the program the ability to introduce and integrate new technologies and architecture patterns while maintaining a secure baseline that meets security standards. These processes are structured to and align with the DevSecOps approach to operationalize evaluation criteria as early in the development process as possible, so as to streamline the delivery process.

To meet this objective, the contractor shall perform the following:

- Develop and maintain an appropriate FISMA level (currently Moderate) of assurance and quality checks within the DevSecOps delivery and release practices and processes. These checks must result in the delivery of all required artifacts necessary to complete standards validation checks (i.e. security compliance).
- Coordinate with the GSA Information Security team often in order to maintain integrated processes that continually meet all necessary security compliance and engineering requirements.

- The TEP must govern approval for all changes to the Cloud Services Authorization to Operate (ATO) within the security boundary.
- Comply with TEP review thresholds:
- Review TEP packages on a quarterly basis to ensure alignment with new templates and to capture changes with the service/product.
    - Ensure components nearing End of Life are planned for future upgrades
    - Review the impact that a Change has so that the required TEP actions appropriate for that change occur (Operational, Minor, Major, Significant).
- Implement and maintain automated test validation checks (i.e. security, operational, etc.) as part of automated delivery activities. (ref: Change Management Testing)

2B 1.4 Sub-objective: Release Management Leadership

Alignment of program vision and strategic initiatives informs direction for the product development while addressing current challenges and opportunities. Lead the definition, measuring of Objectives and Key Results (OKR's) through development of key performance indicators for the portfolio of products and services. Communicate Risks and Issues, and Dependencies across teams by working closely with product delivery teams and coordinating mitigation strategies and resolution. Coordinate intake of new features and enhancements with governance approvals and capacity planning to update product features. Maintain product roadmaps.

The contractor will need to describe their approach to managing legacy products in conjunction with release management of the modernized products. The contractor needs to address options including: 1) an approach that evaluates incoming requests against the existing roadmap for the product and any current operational defects that may need to be addressed, as inputs to the prioritization exercise for the request, as well as; 2) a more modular approach in which releases are much less frequent and take place once cohesive sets of functionality are completed. The contractor must consider factors including technical, budget, schedule, and business drivers.

To meet this objective the contractor shall perform the following:

- Evaluate incoming requests against the existing roadmap for the product and any current operational defects
- Design a modular approach with cohesive sets of functionalities released.
- Plan each Program Increment release with prioritization of incoming New Feature Requests balanced with Program objectives and ensuring adequate capacity to deliver each Program Increment.
- Ensure the Acceptance Criteria (AC) for features is clear and testable so that the functionality can be demonstrated to work in production.
- Demonstrate alignment with each Feature/SRE/Maintenance item of the program increment with the Architecture Roadmap, Objectives, and Key Results of the program.

- Produce release notes, shareable with stakeholders as defined in the Program Stakeholder Management Plan, for each Program Increment and maintenance cycle.
- Update product roadmaps with each release.
- Develop and maintain a code version control strategy, that ensures traceability of changes, and system for both Major (features, updates) and Minor (patches, maintenance) releases.
- Automate notification that a deployment has been completed in the Agile Release management software (currently Jira).
- Document and maintain pre and post deployment process to include:
    - Quality gate thresholds
    - Configuration management and version control

2B 1.4.1 Change Management Testing

We are looking for a contractor to develop and maintain a mature, rigorous testing environment and framework that includes traceability from requirements to the actual tests, testing automation, and reporting of the test results with defined pass/fail thresholds. Where test frameworks may not currently account for certain test cases the vendor must recommend solutions that best integrate tests in a way that reduces human interaction and function necessary to test each change. Finally, if for some reason, automation is not possible the contractor must apply the same rigor to creating and maintaining manual testing.

To accomplish the objective for Change Management Testing the contractor shall:

- Create automated tests for all development work delivered
- Utilize, where possible, available integrations to execute tests automatically as part of the code commit and deployment build processes.
- Develop reusable test cases for each requirement and provide an adequate level of traceability for each test case to the individual requirements, use case, or security control.
- Include and adhere to government approved pass/fail thresholds that identify and automatically stop unacceptable test results from progressing for each test case.
- Include a Test Analysis Report (TAR) with metrics for passed and failed tests for each test and make this report available to government personnel.
- Ensure all materials and code are put into the appropriate configuration management/ release management process for version control and adequate retention after deployments.
- Provide a list of SLA test metrics that will be achieved as part of this proposal.
- Perform automated testing to include but not limited to:
    - Functional testing to ensure all requirements are satisfied
    - Compatibility testing with all interconnected systems
    - Compliance testing with Section 508 of the Americans with Disabilities Act
    - Performance testing

- Regression testing
- Security testing

Where automated tests may not be deemed necessary or viable, as outlined in the Automated Testing sub-section, the vendor shall:

- Account for equally rigorous testing via a manual process. These manual testing processes and procedures, to the greatest extent possible, must integrate manual testing in a way that can regularly reduce human interaction and function necessary to test each change.
- Perform manual testing to account for but not limited to, the following:
  - Validation that any required user documentation is accurately portrayed.
  - Validation that permissions changes maintain anticipated authorization control.
  - Verification that appropriate security controls have been tested and approved.
  - User Acceptance Testing (UAT) (when required).
- Provide a Test Analysis Report (TAR) to the specified Government personnel for each test.
- Transition all materials and code to the appropriate configuration management/ release management process for version control and adequate retention upon government approval of the TAR.

2B 1.4.2 Continuous Delivery

The contractor shall build and deliver application changes using a secure by design framework that considers security requirements early within the release lifecycle during the development phase. Functional changes shall account for standardization and reuse methodology to reduce complexity and streamline efficiency in delivery and maintenance of new application functionality. If the application has a greenfield or application/ data transformation cloud strategy then FAS Cloud Services (FCS) products and services must be used when available to the contractor.

The following considerations shall , at a minimum, be foundational aspects of the secure by design framework developed, implemented, and adopted by the contractor.

- Utilize automated infrastructure as code (IaC) to ensure consistent, repeatable environments
- Utilize immutable infrastructure and frequent (at least once per month) redeployments/restaging to prevent configuration drift
- Implement and maintain automated build processes and delivery pipelines (CD,CI/CD) including functional and security testing, to minimize work in progress (WIP) and consistently ship code to production
- Implement standards around modern, DevOps/DevSecOps, cross-functional, and self-organizing teams and within a collaborative environment where team members have an equal voice

- Include security engineering integrated into the development, test, and production delivery
- Partner with security engineering personnel and processes with every DevSecOps product team
- Utilize compliance engineering practices that can speak in detail to the scope and intent of required security controls. This includes an ability to articulate, in detail, how each control is implemented within the system or integrated systems environment.
- Utilize compliance engineering practices that are integrated with daily application team activities and offer early security requirement coordination and clarification for all technical, operational, and management-based changes or activities.
- Design for and build security control requirements into application requirements
- Define and utilize roles and responsibilities where security is assigned as every team member's responsibility and not separated from the business or development team

The contractor shall leverage the same Continuous Delivery framework for all operational changes to the application in a way that ensures there is no configuration drift introduced through all environments no matter the work performed.

2B 1.5 Sub-objective: Risk Management Leadership

The government is looking to employ a process-driven methodology and common control maturity model that aligns with security frameworks that reduce overall security costs for IT Cloud Applications. Additionally, security activities are focused on minimizing time to market for the FAS business line to achieve Authorization to Operate (ATO) much quicker than traditional approaches. Compliance engineering assists with the development, implementation, and administration of the FCS security program and systems ensure proprietary or confidential data and systems are protected by monitoring, auditing, and enforcing compliance with GSA and FCS Information Security and Information Technology policies, procedures, guidelines, and standards.

To meet these objectives, the contractor shall perform the following:

- Influence the design, configuration, implementation, and test and validation of complex security products, technology systems, services, and infrastructure
- Coordinate vulnerability and patch management to ensure currency and compliance while minimizing attack surfaces, and remediating vulnerabilities in the security program prior to exploit and compromise. Develop technical evaluations to ensure adequate security assessment and screening of vendors and technologies used in the system applications and services
- Coordinate response to Security Advisories, Zero-Day Vulnerabilities and Patches. FISMA Audit Coordination to ensure compliance with the Federal Information Security Modernization Act and obtain an Authorization to Operate.
- Apply Quality Management to improve consistency, repeatability, and predictability of program results resulting in reduced security costs through

improved program processes, performance, automation, and Key Performance Metric measurement
- Perform Continuous Improvement to continually evaluate and set program goals that drive improvements in operational consistency, repeatability, and predictability of program results
- Develop and maintain a Component inventory and management system whereby components reaching End of Life or needing patching will be added to maintenance cycles well in advance of posing any risk to the program
- Provide a lean staff of program support that can be leveraged as shared resources across product and service teams. This may include traditional program management support, such as Program Manager, Finance, Purchaser, Scheduler. as well as more technical/program specific support; such as the leads for technical and data architecture, security, organizational change management/communications, license management, cloud economist, etc.

The contractor shall have a formal Risk Management Board (RMB) and Risk Management Plan (RMP).

- The Risk Management Board (RMB) shall describe the process of identifying, assessing, mitigating, monitoring, and managing risks throughout the entire Program. This RMP and associated processes and procedures are applicable to all organizational levels within the Program. This plan addresses overall program risks as well as risks associated with functional support, projects, cost management, schedule, management, contracts, subcontracts, procurement, and legal. Effective risk management is important for all projects and operational activities conducted across the program, including technical and process improvement projects.

The Risk Management Plan (RMP) shall describe the following:

- How the Program performs risk identification, analysis, management, and oversight for all contractual activities performed by contractor personnel to satisfy the Program requirements identified by GSA.
- Ensure that risks that are common across similar services are identified, mitigated and where applicable, correlated for similarity in approach and mitigation
- Ensure all staff on the project are vigilant for and identify risks.
- Ensure that risks are mitigated at the appropriate level and communicated to the appropriate levels of senior management.
- Maximize use of automated methods to identify potential sources of risk
- Maximize use of automated methods as part of daily work in order to mitigate risks, such as automated code quality analysis in the CI/CD pipeline

The contractor shall have a formal risk management board (RMB) established at the problem level and the service delivery level. To meet this specific objectives and approach, the contractor shall perform the following:

- Update the RMP bi-annually or as directed by the government.
- Ensure that critical risks affecting operations, technical, budget, cost, and/or schedule are proactively identified, communicated, escalated, and mitigated in a timely manner.
- Facilitate attention to key risks affecting the program, projects, service delivery, and other portions of the Program.
- Produce meaningful information that allows program management to focus efforts based on priority of risks (e.g., high likelihood and high impact) through effective coordination of mitigation efforts.
- Ensure that appropriate stakeholders are informed and, if applicable, participate in the risk assessment and mitigation.
- Support standardized and accountable execution of risk management across the program
- Use a risk management strategy that is aligned with the overall Program technical approach and identify actions to minimize risk.
- Support risk management training across the Program.
- Record all risks, risk owners and current status of the risk in a centralized repository accessible to all in the Program.

2B 1.6 Sub-objective: Cloud Tools and Acquisition Management

GSA IT has the responsibility for the development and operation of FCS. Accordingly in that capacity conducts periodic review of system capabilities; including but not limited to software products and subscription services, categorized as Tools, functioning as a part of the service. This review extends to FCS tenants whose application's Tools may impact FCS function. The objective of this review is to assess the appropriateness and viability of continued use, replacement and or removal of a particular Tool in an effort to ensure that FCS functions efficiently, economically and enhances user experience. A listing of Tools currently in use is shown in Attachment 1, Tab M - Technology Inventory of this PWS.

To meet these objectives, the Contractor shall:

- In accordance with the FAR, provide for the timely purchase of Tool renewals according to their individual POP
- Where appropriate and beneficial to the Government, provide for Co-Terming of multiple instance products which are exactly the same.
- In accordance with the FAR, provide for the purchase of new products (not currently in Attachment 1, Tab M - Technology Inventory) at the direction of GSA IT.
- Maintain an inventory of tools purchased for FCS or tenants. Inventory shall be readily accessible to the Government, shall be in sortable spreadsheet format and contain at a minimum the following:
    - Purchased for: FCS or tenant name mnemonic
    - Product Name
    - Manufacturer

    - Provider
    - Provider contact information
    - Indicator of Schedule or open market purchase
    - Product cost at last purchase
    - Description of licensing attributes
    - POP
- Records of specific licensing data, invoices, RIPs or other pertinent information related to the purchase shall be separately maintained and readily accessible to the Government
- Collaborate with GSA IT to make recommendations for additional products supporting Objective 1d, above.

2B.2 Objective 2: Labor Services

2B 2.1 Sub-objective: Cloud Advisory Service

Provides support to application teams through a Cloud Intake process, partnering to develop a cloud strategy/approach for how to deliver value to the business using the GSA IT cloud EcoSystem; it involves development of an architecture, schedule, and budget based on business requirements. Cloud Advisory engages tenants through the Cloud Enablement journey which provides support with a cloud implementation plan, onboarding, and adoption; this includes integrated engineering support for planning and delivery of the application for cloud adoption to achieve minimal viable product (MVP) state. Currently the majority of cloud implementations are using Amazon Web Services (AWS); however, as the organization matures, other cloud platforms such as Microsoft's Azure and Google's Cloud Platform (GCP) will be supported.

2B 2.1.1 Sub-objective: Cloud Intake and Rationalization

Cloud Integration Shared Services (CISS) Advisory Services supports the delivery and maintenance of cloud capabilities to align with the GSA IT vision and improve software development for the GSA's IT organization. CISS is a mission focused program and is paramount to the success of the tenant teams' planning to develop and execute a cloud modernization and transformation strategy.

CISS Advisory Services, in terms of enterprise cloud strategy alignment, enterprise cloud enablement process enhancement and GSA IT cloud transformation and modernization promotion, standardization and governance, is essential and critical to the success of GSA IT.

At the Strategy Level, the contractor shall perform the following:

- Provide expertise and guidance toward cloud strategies, overall agency cloud portfolio, and long-term goals.
- Identify and develop a mature and persistent cloud rationalization processes/approaches and report successes of cloud adoption at an agency level
- Leverage Rationalization methodologies such as TIME (tolerate, invest, migrate, eliminate) analysis.

- Conduct ongoing review and assessment of capabilities and services in multiple cloud environments leveraging the results as part of the advisory service and provide recommendations to approved cloud services.
- Perform assessments to evaluate the various cloud offerings, from private, public, and hybrid cloud providers with the goal of enabling IT solutions to support the infrastructure, application, security, and operations needs. multi-cloud offering to support IT solutions while identifying private, public and hybrid cloud mix across infrastructure, application, security and operations.
- Create and support the documenting of enterprise IT cloud strategies through concept papers and white papers when newly identified/built capabilities are incorporated into the cloud service offering
- Contribute to, support, develop, update, maintain GSA IT playbooks, cloud strategy, cloud transformation reference architectures, common architectural macro and micro patterns, and associated rationalization and applicable scenarios.
- Advise, support, develop and implement enterprise IT strategies and processes of new technologies adoption; support in developing strategic vision of short- and long-term enterprise IT cloud asset roadmap.
- Advise, develop, enhance, improve and implement cloud enablement stakeholder engagement and management processes and procedures to achieve high efficiency and scalability.
- Create guidelines, questionnaires, assessment matrix and guides related to cloud readiness.
- Assess enterprise cloud adoption challenges; advise, develop and implement solutions to solve these challenges.
- Develop comparison tools and guidance recommendations between optional hosting environments such as on-premise versus agency cloud hosting.
- Identify and advise deliverables for business evaluation, technical evaluation, and budget evaluation for cloud deployment or migration.
- Define and report metrics of success and value derived from cloud deployment, migration, and ongoing iterative transformations.
- Support agency efforts for training in cloud related technologies and best practices. Advise, support and construct agency cloud awareness programs and frameworks.
- Assist in cloud procurement activities, such as cost estimation, TCO, cost/benefit analysis and comparison.
- Provide a GSA IT wide cloud intake and strategy development framework that coordinates, advises and enables GSA IT wide stakeholders with cloud initiatives and investments.
- Develop cloud services, standards and automation delivering more repeatable and reusable cloud shared services to reduce overall engineering, operations and support schedules and costs.
- Provide a standardized way to report cloud economics that provide greater insight into cloud related spend, avoidance / savings opportunities delivering the greatest value to GSA IT.

At Technical and Operational Level, the contractor shall perform the following:

- Assist the agency in execution of proofs of concept (POCs) and prototypes to explore and develop cloud services and cloud architectures.
- Lead and/or assist, as required, in designing and developing reusable components for cloud environments.
- Contribute to more consistent requirements development for existing GSA cloud services and processes in order to build upon and account for the current design patterns and deployment methodologies via IT Playbooks.
- Contribute to reusable cloud capabilities requirements using secure-by-design frameworks to assist in providing guardrails and playbooks for application teams where existing GSA cloud service adoption may be lacking.
- Support the adoption of existing GSA Cloud Services.
- Maintain roadmap of available GSA Cloud Services, including associated tenants looking to leverage these services.
- Identify divergence in approaches, and adoption of GSA Cloud Services within applications cloud reference architecture.
- Maintain a cost model that provides transparency in rate/volume that each client has consumed for each service(s).

In addition to refinement of GSA IT enterprise cloud strategy, it's equally important to support early tenant engagement and on-boarding during cloud adoption.

To meet this objective, the contractor shall perform the following:

- Assist, contribute and support, if necessary, in developing and reviewing GSA IT Business System technical documentation that may be part of, or contributing towards, IT Playbooks and pre-solicitation reference materials.
- Assess existing applications, systems, and/or any IT assets to determine their readiness to be migrated to a cloud computing environment, based upon factors such as privacy, security, performance, and service level agreements.
- Create target technical recommendations by evaluating business requirements for applications or workloads and mapping to agency cloud offerings for cloud selection.
- Perform cloud adoption and capability alignment to assess tenant current situation and create a roadmap with short-term, mid-term and long-term goals to help maximize tenants cloud foundation and cloud potential.
- Perform cost-benefit analysis and calculate return on investment (ROI) of tenant's cloud migration.

2B 2.1.2 Sub-objective: Cloud Economics

In order to effectively manage costs, staff productivity, operational resilience and business agility and capture Total Cost of Ownership (TCO), the Program and Tenants need to have a transparent view of cloud consumption. Cloud Economics provides the means for tracking, reporting, predicting, and sound decision-making.

To meet this objective, the contractor shall perform the following:

- Maintain individual tenant spending on all cloud services provider (CSP), to include
    - Provide a Tenant Monthly Usage Report (Attachment A, Tab G – Tenant Invoice), to each tenant on a monthly basis following consumption of services
    - Provide a Tenant Self-Service portal with near-real time details on cloud spend being consumed
- Maintain the proportional ratios for spending that is considered an operating expense (how much a tenant would use of resources/services that don't have the ability for tenant's specific attribution)
- Provide frequent technical recommendation reports of how to optimize CSP spend.

  Examples include, but are not limited to:
    - Identify underutilized and overutilized resources
    - Identify resources mismanaged (patterns in use of on demand or keeping resources operational when not needed)
    - Identify resources that would perform more effectively within the budgets (i.e. X M4.large could perform more efficiently with x M5.Xlarge for x service)
    - Identify resources not authorized to use
    - Identify resources used in non-US regions
    - Identify resources that did not take advantage of scaling capabilities
    - Identify zombie/idle resources
    - Identify cold data that can be moved to cheaper storage tiers
- Provide saving opportunities to the Cloud Advisory/Cloud Enablement teams, to each of the product/service owners and monthly cost advance meetings (Part of Monthly reporting)
- Develop a Cloud Economics Model applicable to GSA IT to evaluate Cost Savings and Avoidance, Staff Productivity, Operational Resilience and Business Agility, referring to an AWS Cloud Value Framework.

2B 2.2 Sub-objective: Cloud Enablement Services

GSA IT has invested time and effort to operationalize a Cloud Enablement strategy that serves as the methodology for its end-to-end Product Development Lifecycle. This governance evaluates the overall technology strategy and how to recommend investments to provide new shared services for GSA IT. This Cloud Enablement team collaborates, engages, consults, and supports each other, through partnership, in developing shared strategic goals and objectives to achieve successful cloud adoption within the Cloud Services EcoSystem.

FCS supports the delivery and maintenance of cloud capabilities to align with the GSA IT vision and improve software development for GSA business systems. FCS is a mission supporting program and is paramount to the success of the applications teams' planning to develop and execute a cloud modernization and transformation strategy.

Cloud adoption, in terms of early engagement[4] and on-boarding support as they relate to cloud strategy, is essential and critical to the success of GSA IT.
To meet this objective, the contractor shall perform the following:

- Advise, recommend, and support GSA IT applications that outline how FCS can best support cloud modernization and transformation strategies.
- Develop and support cloud enablement processes that foster quality in service-provisioning and include continuous improvements to the program.
- Contribute to requirements development for FCS processes and services in order to build upon and account for the current design patterns that the IT Architecture and Engineering group outlined. This is to drive more consistent development and deployment of valuable business functions for FAS.
- Enhance capabilities, within secure-by-design frameworks, to assist in providing guardrails for cloud application development teams where FCS service adoption may be lacking.
- Support the adoption of FAS Cloud Services.
    - Maintain roadmap of available FAS Cloud Services, including associated tenants looking to leverage these services.
    - Identify divergence in approaches, and adoption of FAS Cloud Services within applications cloud reference architecture.
- Maintain a cost model that provides transparency in rate/volume that each client has consumed for each service(s).

Consistent processes and operations are essential to application modernization with services provided.

The contractor shall:

- Improve outcomes for clients by transforming legacy, monolithic systems into modern architectures based on modular elements and microservices.
- Implement lean development practices, continuous delivery pipelines, and automated functional and security testing to shorten cycle times, reduce Work in Progress (WIP), and quickly and consistently deliver code to production within a large enterprise.
- Organize operations around a modern Site Reliability Engineering (SRE) model that sets, monitors, and achieves Service Level Objectives (SLOs) while reducing time spent on manual or toil tasks.

2B 2.3 Sub-objective: Cloud Compliance Services

Security and compliance requirements are a shared responsibility between the CSP and the consumers of cloud services. Within GSA this shared responsibility is further refined between several stakeholders such as the CISS/FCS, System/App teams, GSA IS, and the Privacy Office. This contract shall require a close partnership with GSA Information Security teams in order to develop innovative compliance models in areas such as; risk

[4] https://sites.google.com/a/gsa.gov/fas_it_playbook/it-playbook/fas-cloud-services/enablement

management and remediation, security control documentation, compliance readiness reviews, Authority to Operate (ATO), Identity and Access Management (IAM) and the associated roles and responsibilities within each area of compliance. The FCS assigned Information System Security Officer (ISSO) shall be responsible for all role responsibilities as outlined within GSA's CIO P 2100.1 policy (See Section 8.4 "Safeguarding Sensitive Data and Information Technology Resources").

As new and existing tenants receive security support via the FCS Cloud Acquisition Tools (CAT). CAT is a FISMA System of Systems that oversees the adoption of the cloud compliance framework for tenants and ensures they understand and plan for required security considerations. The contractor shall maintain process management and status reporting for FCS CAT tenants as they onboard and adopt cloud services. The CAT assigned ISSO shall also be responsible for security responsibilities related to CAT and CAT sub-systems per System security requirements required per GSA's OCIO p 21001.

Both the FCS and CAT ISSO's shall maintain an ISSO Compliance Handbook of key processes and procedures that outlines support for the following:

- Coordination and Approach to Risk Management
- Risk Tracking and Remediation Activities
- Weekly Security Scorecard Reporting
- Training Requirements and Activities
- Internal Operational Audits and Reviews
- TEP Integration and Participation

2B.3 Objective 3: Technical Services

It is imperative that modern IT Systems deliver both quality and security as a foundational aspect of their delivery. Security should go hand in hand with development and deployment, and be part of ongoing operations and maintenance. We envision structuring teams around products that are shared across the enterprise. The teams are diverse, encompassing the business, IT, and security staff. All technologies are grouped into specific products and to address a capability. If not explicitly stated otherwise, All services/technologies shall apply the following Subtask 3.1: Software Development and Coding Practices, Subtask 3.2: DevSecOps Framework and Subtask 3.3: Building Cloud Native.

Additionally, the below listed cybersecurity considerations shall be accounted for across all services/technologies.

Binding Operational Directives (BODs)
The Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS) develops and oversees the implementation of "binding operational directives" and "emergency directives," which require action on the part of GSA to effectively manage and comply with. The following policies require consideration with how they are achieved with the services and support defined in this statement of work.

- BOD22-01- Reducing the Significant Risk of Known Exploited Vulnerabilities
- BOD20-01 - Develop and Publish a Vulnerability Disclosure Policy
- BOD19-02 - Vulnerability Remediation Requirements for Internet-Accessible

Systems
- BOD18-02 - Securing High Value Assets

CyberEO Specific Office of Management and Budget (OMB) Policy
- OMB M-21-30 - Protecting Critical Software Through Enhanced Security Measures
  - Key Mandates: Inventory critical software, follow NIST guidelines for implementation of controls to protect critical software
  - Key Timelines: Controls must be in place by 8/10/22
- OMB M-21-31 - Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents
  - Key Mandates: Executive Order for logging, log retention, and log management, with a focus on ensuring centralized access and visibility for the highest-level enterprise security operations center (SOC) of each agency. 30 months of log storage (12 months hot, 18 months cold), full stack/all tool logs centralized, full packet capture stored for 72hrs,
  - Key Timelines: FY22 Q1 Increasing log retention timeframe, FY22 Onboarding application, db, and tool logs (fully stack logging). Maturity Level EL1 by August 2022; Maturity Level EL2 by February 2023; Maturity level EL3 by August 2023
- OMB M-21-XX (Currently in Draft) - Moving the U.S. Government Towards Zero Trust
  - Key Mandates: Enterprise ICAM, MFA, Encryption in transit, Applications treated as internet accessible (Zero Trust), Data protection controls in place. Alignment to agency ZTA plans.
  - Key Timelines: Required actions integrated by the end of FY24

FCS operates as a product team program for planning and executing operational activities under the DevSecOps framework. Under this framework it is necessary to understand that within FCS operations there is no separation or differentiation between traditional operations, service support, minor enhancements, or bug fixes.

To meet this objective, the contractor shall perform the following:
- Communicate in advance, to the greatest extent possible, all partial and full impacts to tenant products or services and workload environments (per FCS Service SLA).
- Operate FCS product and services teams utilizing a Service Reliability Engineering (SRE) model that sets, monitors, and achieves Service Level Agreements (SLAs) while reducing time spent on manual or toil tasks.
- Define and document service level objectives(SLO) for the service capabilities and report the SLO to internal tracking and tenant provided event monitoring where necessary

- Coordinate and align SRE actions and activities within the FCS product team velocity.
- Coordinate incident response to FCS Services between SRE members for each product and services team in a way that expedites partial and/or full outages to minimize tenant downtime to the greatest extent possible (per FCS Service SLA).
- All components/technologies for a service comply with the following
    - End of life (EOL) software is updated/upgraded within SRE
    - Patching and or Implementation of security migrations are completed within Attachment 1, Tab H - Performance Measures.
    - Packages / scripts / templates are maintained / updated for any changes
- Product / Service are leveraged by a baselined application ("Hello World") for verification the SLO are met and any application user can see how basic use of service is defined via code

2B 3.1 Sub-objective: Software Development and Coding Practices

These are the general design principles and practices that are part of any solution or managing the entire program. This section will break apart several areas to support the following objective.

To meet this objective, the contractor shall perform the following:

- Codify the deployment of all cloud services and infrastructure using Infrastructure as Code best practices (including using declarative syntax and idempotency), where technically feasible, achieving zero configuration drift within all supported environments and deployments.
- Ensure that all services/projects developed use a version-controlled repository, maintain all dependencies via a package manager or equivalent automation, leverage resources provided by services (Unmanaged, Semi-Managed, Fully Managed), where possible, and have an SOP developed throughout development to include, but not limited administration, tenant support, patching, and/or upgrades
- Create a testing plan, perform benchmark and load testing, deliver the system performance benchmark matrix (ref: Change Management Testing) and develop Unit/Integration testing for all services/projects to thoroughly test all critical business logic.
- Design single-purpose modular, configurable, extensible and composable software modules, libraries, and components ensuring that all code is idiomatic, follows the playbook for the respective language and adheres to the DRY (don't repeat yourself) concept

[5]

- Instrument metrics, logging and tracing in all developed code and integrate with the centralized logging and monitoring solution to improve debuggability, operational awareness and root cause analysis.
- Create and present demonstrations of code, features, and software as required by the government for approval by the government point of contact
- Leverage the standard deployment process

To meet this objective, the contractor shall perform the following:

- Create and /or leverage the CI/CD Service to support modern software development patterns where it applies, this is the standard deployment process.
- Services are deployed in small frequent updates (leverage the continuous integration and continuous delivery service)
- Streamline the processes of delivery and deployment
- Leverage immutable infrastructure and frequently redeploy/restage to prevent configuration drift
- Automate builds with integrated and security testing
- Keep change log and SOPs updated for reference in a centralized repository

2B 3.2 Sub-objective: DevSecOps Framework

It is an absolute necessity for the contractor supporting this Task Order to account for and deliver quality and security as a foundational aspect of their delivery. In order to accomplish this the contractor shall support the following items as foundational considerations when building and delivering the responsibilities outlined within this TO.

- Improve outcomes for clients by transforming legacy, monolithic systems into modern architectures based on modular elements and microservices.
- Implement lean development practices, continuous delivery pipelines, and automated functional and security testing to shorten cycle times, reduce Work in Progress (WIP), and quickly and consistently deliver code to production within a large enterprise.
- Organize operations around a modern, Site Reliability Engineering (SRE) model that sets, monitors, and achieves Service Level Objectives (SLOs) while reducing time spent on manual or toil tasks.

It is imperative that modern IT Systems deliver both quality and security as a foundational aspect of their delivery. Security should go hand in hand with development and deployment and be part of ongoing operations and maintenance. CISS envisions structuring teams around products that are shared across the enterprise. The teams are diverse, encompassing the business, IT, and security staff.

To meet this objective, the contractor shall perform the following:

- Engineer and maintain cloud services to support lean development practices, continuous delivery pipelines, and comply with the Change Management Testing

- Help shorten cycle times, reduce Work in Progress (WIP), and quickly and consistently deliver applications to production.
- Build, deliver, and maintain FAS Cloud Services changes using secure-by-design frameworks that consider security requirements early within the release lifecycle and during the development phase.
    - Organize around modern DevOps/DevSecOps teams in a collaborative environment
    - Adopt agile development method and leverage ChatOps for internal/external collaboration and support pilot tenant applications onboarding.
    - Institute compliance engineering that articulates in detail the scope and intent of required security controls, including how each control is implemented within a system or integrated into the environment
    - Help establish, chart, govern, and participate in the Technical Evaluation Process (TEP) and the Change Control Board (CCB)

To properly control and assess technical changes and enhancements to the cloud environment the FCS has implemented a Technical Evaluation Process (TEP), which is an enforcement gate for the necessary information to evaluate for possible impact prior to production deployment. These processes are structured to, and align with, the DevSecOps approach to operationalize evaluation criteria as early in the development process as possible, so as to streamline the delivery process.

To meet this objective, the contractor shall perform the following:

- Develop and maintain an adequate level of assurance and quality checks within the DevSecOps delivery and release practices and processes. These checks must result in the delivery of all required artifacts necessary to complete standards validation checks (i.e. security compliance).
- Coordinate with the GSA Information Security team in order to adequately maintain integrated processes that continually meet all necessary security compliance and engineering requirements.
- The TEP must govern approval for all changes to the FCS Authorization to Operate (ATO) within the security boundary.
- Automated delivery activities comply with the Change Management Testing

2B 3.3 Sub-objective: Building Cloud Native

The journey to cloud is not about IT infrastructure, it's about working with the business systems to help transform the business. Our goal is not lift and shift, we strive to build cloud native solutions in order to improve efficiency, scalability, and resilience. Ultimately, the journey to cloud must come with better performance and greater business value.

To meet this objective, the contractor shall perform the following:

- Build and design new shared service offerings to support multi-tenancy, API-based consumption and issuance, modularly, configurability, and extensibility.

- Leverage immutable infrastructure and frequently redeploy/restage to prevent configuration drift
- Containerized workloads, when technically possible, to maximize scalability and portability
- Seek standards-based solutions with a preference toward open standards and architectures over closed and proprietary ones
- Define KPIs for the journey to cloud to ensure that we are realizing the benefits and not just migrating for the sake of migrating
- Solutions resilient and respond to demand changed with providing changing resources to stay within SLO without human intervention
- Solutions loosely coupled and each microservice deployed independently
- Microservices comply with semantics versioning, each can be deployed, scaled restarted independently from other microservices
- Provide the Analysis of Alternatives with each technical change with a consideration for total cost of ownership from three perspectives, “Buy, Build or Reuse” any technology or service.
    - Buy: Leverage a managed service that requires minimal customer responsibility to use.
    - Build: Provide a solution and all requirements to use service, including the highest responsibility of the entire solution
- Reuse: Leverage the services that are in use and require a specific amount of responsibility to operate.

2B 3.3.1 Sub-objective: Unmanaged IaaS

Unmanaged Services - This is the most basic cloud foundation service which provides quick access for development teams (Tenant) to build their own solution. This cloud foundation should also deliver the core infrastructure necessary to support the Semi-managed and Fully-managed products and services. This comes with minimal inheritance of security controls; the Tenant has full responsibility for obtaining an Authorization to Operate (ATO).

These services shall provide application teams significant flexibility and the ability to own nearly everything related to their cloud solution. Application teams can build their own toolings and own their software delivery processes. This is considered an option when an application team cannot operate within the managed services due to a technical risk.

To support these products and services the contractor shall provide:

- An On-demand number of virtual private cloud for a tenant/application team
- Access to the tenant with an account for them to directly provision and configure their environment.
- No monitoring, testing, security, etc.
- Consumable standardized Infrastructure as Code (IaC) fabric such as, but not limited to, Terraform modules and Ansible roles. Consumption of these modules and/or roles is optional.

Any development or configuration above/beyond in the tenant VPC environment shall be done via add-on professional services or provided back by the tenant via the contribution model.

- FCS: sets up networking so tenants can integrate with other cloud services.
- Tenant: provisions and configures cloud tools and services as they see fit
- Chargeback: tenants pay by account (one account per VPC) – account is a pass through for AWS services (pay by consumption).
- Provide support for tenant isolation and support multi-tenancy reducing security risk, improving usage-based billing, and delivering maximum customer flexibility and configurability.

2B 3.3.1.1 Sub-objective: Cloud Networking

Cloud networking is the communication backbone of FCS. The FCS Network is built entirely on AWS. The architecture is centralized by a transit VPC that hosts all key network components. Tenant VPCs and accounts, GSA on-premise, and internet access are connected to this centralized network VPC.

The contractor shall:

- Automate using infrastructure as code as stated in Building Cloud Native Objective
- Maintain, configure, and support the following (but not limited to): Cisco CSR, Route53, Route53 resolvers, AWS transit gateway, AWS security groups, Citrix Netscalers, Nginx load balancing, AWS load balancers (ALB, NLB) and SSL termination
- Proactively identify and communicate issues and risks to government leads, including impact, severity, and mitigation plans
- Proactively investigate and recommend areas of improvement to help overall performance of the FCS platform
- Troubleshoot, resolve, and support all network operational disruptions, degradation, and outages
- Provide a root cause analysis for all outages and degradations within 48 hours of the outage resolution
- Perform and support all migration efforts such as but not limited to migrating Trend Micro policies to AWS security groups and migrating Netscaler ADC to Nginx
- Regularly upgrade software to the latest version following FCS procedures in sections Technical Evaluation Process (TEP) and the Change Control Board (CCB)
- Create and deliver technical SOPs for any new FCS network services
- Update technical documentation when any change is made to an FCS network service
- Perform all agile scrum ceremonies, including sprint reviews and daily scrum

- Use FCS ticketing systems to track all incidents, change requests, user stories, defects, and other tasks

2B 3.3.1.2 Sub-objective: Cloud Identity

The FCS IDMS provides authentication and authorization services for the FCS platform to comply with GSA Security standards. FCS IDMS unifies various Identity Management components and manages them from a central location. It allows users to have a single account for all platform access. All accounts conform to all GSA Information Technology policies and mandates.

The contractor shall:

- Automate using infrastructure as code as stated in Building Cloud Native Objective
- Maintaining, configure, and support the following (but not limited to): ForgeRock identity management and directory products, LDAP, Active Directory, Windows policies, OpenUnison, Okta, AWS access keys, AWS KMS, AWS IAM, AWS IAM policies, SAML and OAuth
- Update, Maintain, configure, and support ForgeRock identity management and directory products
- Perform regular patching and maintenance of all FCS virtual hardware that the IDM and directory systems run on and the all-IDM specific software
- Proactively investigate and recommend areas of improvement to help overall performance of the FCS platform
- Automate and support infrastructure as code using but not limited to Ansible, Terraform and CloudFormation for all aspects of IDM and directory services (account provisioning, system management, patching, etc.) to ensure consistent, repeatable environments and procedures
- Troubleshoot, resolve, and support all IDM and directory services operational disruptions, degradation, and outages
- Complete a root cause analysis for all outages and degradations within the time allotted within the Quality Control Plan and respective performance measures.
- Perform and support any migration efforts to new IDM solutions
- Regularly upgrade software to the latest version following FCS procedures in sections Technical Evaluation Process (TEP) and the Change Control Board (CCB)
- Create and deliver technical SOPs for any new FCS IDM services
- Update technical documentation when any change is made to an FCS IDM service
- Perform all agile scrum ceremonies, including sprint reviews and daily scrum
- Use FCS ticketing systems to track all incidents, change requests, user stories, defects, and other tasks

2B 3.3.1.3 Sub-objective: Cloud Infrastructure

GSA is developing a standardized, cloud-based Infrastructure as a Service (IaaS)

with automation, value description, and a clear delineation of responsibilities between IaaS providers and tenants as its foundation. In combination with Advisory Service, Security Service, and Network Service, IaaS promises to increase cloud adoption at GSA. This foundational cloud service will be repository-centered, and Infrastructure as Code (IaC) focused on increasing flexibility and efficiency.

To meet this objective, the contractor shall perform the following:

Development:

- Leverage legacy architecture and automation [existing code base includes, but is not limited to, the following languages: Golang, Terraform/HCL2, Python and Ansible]
- Identify synergy between FCS architecture and other GSA IT infrastructures
- Extend existing capabilities to build the foundational IaaS offering
- Create or improve services based on customer and business requirements to be configurable, modular, extensible, consumable, and cost-effective for GSA and its customers.
- Develop thoroughly tested IaC and serverless solutions for managing infrastructure assets, where possible, to increase consistency, reliability, availability, and auditability.
- Provide an IaaS capability that supports maximum customer isolation, flexibility, and configurability
- Create single-purpose, configurable, reusable, flexible, and version-controlled modular components
- Define and document a standardized testing framework for all modular component types to maintain code quality, standards, and security
    - Enhance and maintain the CSP account policies to maximize the consistency and automation of cloud governance for each tenant, including the ability to provide tenants the security-approved cloud services available through the CSP.
    - Collaborate with MCaaS to maximize the secure containers offered to both tenants and shared services.
    - Review and recommend cost-cutting technologies and methods to increase efficiency and reduce infrastructure’s overall operations and maintenance cost.
    - Develop and maintain Security as Code and Automated Assessment Code as needed by the solution.

Operations:

- Lead refinement and iterative updates to ensure the accuracy of IT Cloud playbooks, guides, best practices, standards, patterns, diagrams, and technical documentation as needed.
- Collaborate with Advisory Service to establish and maintain tenant communication and education through documented SOP, RASIC, IaaS product roadmap.

- Contribute to, participate in, and lead, as necessary, ritual meetings, pairing sessions, demonstrations, presentations, and design meetings on a team using Lean Agile, Agile, and DevSecOps methodologies and patterns.
- Contribute to third-party open-source repositories, as necessary, to add features, functionality, or bug fixes to tools used by the System.
- Collaborate with Advisory Services to establish or enhance the intake process and the IaaS showback and chargeback cost model.
- Develop a transition plan for existing AWS Systems and VPCaaS tenants into the IaaS.
- Coordinate with the Network and Security services to ensure the IaaS environments are secure.
- Coordinate with the Network Service and the CSPs to provide high bandwidth connectivity to GSA on-premise and other CSPs.
- Develop, maintain, and share best practices for efficiently managing production workloads.
- Collaborate with Advisory Service to gather customer satisfaction data, feature requests, client satisfaction, and value metrics to inform the IaaS product roadmap and increase tenant satisfaction.

2B 3.3.1.4 Sub-objective: Use of IPv6

GSA expects to effectively provide assurance for its users that services and service elements (technical, management and operations-related) acquired will be in compliance with national policy throughout the life of the contracts. The contractor shall ensure that services delivered are in compliance with national policy directives that apply to the national telecommunications infrastructure. Specific national policy requirements include, but are not limited to:

- 1. OMB Memorandum M-21-07 directs that agencies must transition from IPv4 agency infrastructures to IPv6 agency infrastructures (network backbones). For agencies with an IPv6 network (and those implementing IPv6 networks) the contractor solution must maintain functionality and shall comply with relevant policies and standards defined by OMB and NIST.

The Contractor shall submit evidence that proposed modernized improvements are in compliance with IPv6-only standards in accordance with FAR 11.002(g) to the Contracting Officer for evaluation for any information technology (IT) that will have the capability to access the Internet or any network utilizing Internet Protocol. Evidence may include any of the following:

i. The Supplier's Declaration of Conformity (SDOC). The template for the SDOC can be found on the National Institute of Standards and Technology (NIST) website available at https://www.nist.gov/programs-projects/usgv6-program;
ii. Laboratory Certification. The product being acquired has been tested and shown to be IPv6 compliant by an accredited laboratory. A listing of tested/certified products can be found on the NIST available at https://www.nist.gov/programs-projects/usgv6-program;

iii. Practical Demonstration. The product can be shown to the *[agency name]* Chief Information Officer (CIO) or designee to be IPv6-only compliant via practical demonstration, or by an otherwise credible validation of technical support; or
iv. If any of (i), (ii), or (iii) is not practical or would pose undue burden on an acquisition action, the CIO may waive this requirement but will require documentation from the contractor detailing explicit plans including but not limited to timelines to incorporate IPv6 only capabilities to their offering.

2B 3.3.2 Sub-objective: Semi-Managed IaaS

This service option provides Tenants with some guardrails and basic services allowing them to inherit a greater set of security controls for their ATO. These products are structured for specific capabilities. Those generally require the application/tenants to configure and manage all integration of those capabilities. These are for application teams with a unique risk that prevents aligning with the GSA IT Playbooks for specific design patterns.

They provide access to capabilities with specific guidance on how to consume the service. Provides services to the application/tenant teams to focus on business functionality and reduce operational maintenance associated with managing “below the line” technologies to support contestant deployments to production.

All services or tooling shall:

- Follow the Cloud Enablement process for evaluating how the service needs to provide the service or met the specific service level objectives
- Leverage Unmanaged service offerings where practical and efficient to maintain and inherit defined standards in these foundational offerings.
- Provide support for tenant isolation and support multi-tenancy reducing security risk, improving usage-based billing, and delivering maximum customer flexibility and configurability.

2B 3.3.2.1 Sub-objective: Semi-managed Containers (CaaS)

The FCS Container as a Service (CaaS) offering provides tenants with a comprehensive application delivery platform by providing containerization alongside resources for building, delivering, and maintaining a scalable, resilient application without having to manage infrastructure.

Provide a capability for a specific tenant to deploy containerized services.

All products, capabilities, or tooling used to support CaaS shall:

- Be efficient and develop reusable components to provide automated self-service capabilities to tenants where possible.

- Maintain and create CaaS documents to match with the latest states
- Support and maintain the current service in accordance with SLAs defined in Attachment 1, Tab H - Performance Measures
- Provided recommendation to Cloud Advisory/Enablement on how CaaS can be supported by MCaaS.
- Develop recommendation and support migration of the service to MCaaS.

2B 3.3.2.2 Sub-objective: API Framework

Cloud Integration Shared Services (CISS) API Management framework supports the delivery and maintenance of API Products to align with the GSA IT vision and improve software development for the GSA's IT organization. CISS is the GSA IT Cloud division and is paramount to the success of the application teams' planning to develop and execute API Management as part of their modernization and transformation efforts.

CISS API Management framework, in terms of enterprise cloud strategy alignment, develops, manages and maintains API process and technology supporting GSA IT cloud transformation and modernization through the promotion, standardization and governance that is essential and critical to the success of GSA IT.

To meet this objective, the contractor shall perform the following:

- Analyze, collect and document all API business requirements and technical conditions, including data access needs, data protection and management policies and security standards along with permissions and authentication.
- Review development environments to identify and remedy needless complications and inefficiencies.
- Create and assist in API development, API testing and deployment using an agile approach and API performance statistics approved and monitored by the GSA IT for each item.
- Identify, implement, support and manage API integrations for applications and services, governance controls, design specifications, lifecycle management, catalogs and portals, and workflows to improve efficiencies
- Identify and reduce duplicative implementations
- Control, facilitate the interactions and communications between API developers and application product owners to ensure that new or re-created APIs have optimal scalability, performance and dependability and conform to agency standards and security guidelines
- After deployment, lead efficient API management, make upgrades and changes as needed to maintain a current, secure, and available solution.
- Lead development and design of API documentation website pages using HTML, CSS, and markdown. Manage source code workflows, repositories, and permissions via GSA identified solutions.
- Provide consultation on best practices via training, writing articles and playbooks, and other methods.

2B 3.3.2.3 Sub-objective: FCS Data (FCS-D)

FAS Cloud Services - Data (FCS-D) a set of specific data services from the FAS Cloud Service EcoSystem that are focused specifically around the data. FCS-D is focused around enabling several data services to provide the Acquisition Workforce (AWF) to study, research, analyze, or collaborate on FAS systems data. FCS-Data is part of the larger FAS Cloud Service EcoSystem and focused on providing a "Centralized Data Analytical, Service Wide Coordinated Capability". FCS-D has defined seven services that provide the ability for Application Modernization and the Acquisition Workforce the means to conduct their mission. FCS Data (FCS-D) supports the delivery and maintenance of Data Analytical products and services to align with the GSA IT vision and improve the tenant development experience. The semi-managed data analytical products include but are not limited to Data Warehouse, Data Lake, Data Transformation (ETL) and Business Intelligent(BI) tools. The FCS-Data capabilities have 3 major types of labor:

- SRE (Service Reliability Engineer) Labor Support
- Professional Services to use the existing capabilities/Services for the existing and future FCS Data tenants.
- Develop New Capabilities/Services Delivery and implementation.

Developing, executing, and maintaining all the data services which are currently in development, test, stage, and production while new services/capabilities are to be implemented.

To meet this objective, the contractor shall perform the following:

- Data Transformation - Developing and maintaining existing Extract, Transform, and Load (ETL) Procedures.
- The professional services support over 65 ETLs for maintaining 38 data sets and collections of corporate reporting as well as visual dashboards for several Tenants.
- All work adheres to the vision from GSA's Chief Data Officer (CDO) and FAS Data & Evidence Governance Board (DEGB).
- Data Management, Data Visualizations, Business Intelligence (BI), and Data Migration Service (AIR- Application Integration repository)
- Establish and maintain the data governance policies, data custodians roles and responsibilities and as well as data operation maintenance policy.
- Contractors must have the latest knowledge and experience of ETL tools defined in Attachment 1, Tab M - Technology Inventory and best practices and provide aggressive and obtainable feature updates.
- Must adopt changes or additions in relevant policy and guideline requirements (Section 8.4)

2B 3.4 Sub-objective: Fully-Managed PaaS

Fully-Managed Services - This service option provides a sophisticated suite of services for the Tenant, allowing them to focus on the application development and delivering

business value as well as an accelerated ATO process.

Offerings at this level provide the highest ATO control coverage and the least tenant responsibility. FCS provides enhanced support services to facilitate the day-to-day operations and maintenance of the underlying infrastructure on behalf of the tenant.

Modular and multi-tenant services at this level are made available as required by the government to support tenants at lower levels in further reducing the burden of hosting cloud services and systems.

The contractor shall perform the following:

- Follow the Cloud Enablement process for evaluating how the service needs to provide the service or met the specific SLO's
- Leverage Semi-managed service offerings where practical and efficient to maintain and inherit defined standards in these foundational offerings.
- Continue reduction of security risks, improving usage-based billing, delivering maximum customer flexibility and configurability.
- Maintain existing shared libraries used in CI/CD pipeline
- Maintain, configure, and support the following (but not limited to): Splunk, AWS CloudWatch, AWS CloudTrail, SensuGo, ElasticSearch and Datadog

2B 3.4.1 Sub-objective: Compute Stacks (EBTA)

Everything but the App (EBTA) offers multiple stacks along with respective architectures. Tenants are not responsible for any part of the infrastructure.
Tenants are only responsible for re-deploying the stack within the maintenance cycle or as they deploy new code into production. EBTA inherited between 70% and 80% of the security related controls which minimizes the concentration of Security needed for the application.

In addition to the preconfigured stacks, some of the core tools listed here shall be available to EBTA tenants for application deployment as part of the service functionality.

- GitHub: deliver source codes repository
- Jenkins: used to launch parameterized jobs to perform allowed stack operations
- Artifactory: for staging purpose
- S3 portal: a user interface that allows S3 bucket access without the need of AWS console
- Splunk: used to view log files associated with a given stack
- Data Jumpbox: used to access database with data tools loaded in the box

The contractor shall:

- Maintain and create EBTA documents to match with the latest states

- Support and maintain EBTA stacks and clean up no longer needed EBTA resources
- Provide advisory support in order to migrate to MCaaS platform

2B 3.4.2 Sub-objective: Application Optimization Services (caching, streaming, etc.)

Application Optimization Services provide real-time analytics and caching capabilities, which allow applications to persist data and retrieve data with high throughput and low latency. These services include but are not limited to AWS managed MemCache as part of EBTA compute stacks, AWS managed ElastiCache/Redis, SQS, SNS and MSK as part of the MCaaS EcoSystem.

The contractor shall:

- Maintain, enhance and optimize the code quality and operational efficiency of all subcomponents and features of these services.
- Maintain and update relevant portions of MCaaS product documental portal related to these services to ensure it's up to date at any given time.
- Participate in, contribute to and lead as required in architectural design, review and engineering of standardizing and extending these services to align with the shared service model to support semi-managed and fully-managed environments which includes non-MCaaS tenants.
- Support Cloud Advisory Service identifying new opportunities for augmentation of Application Optimization Services. Contribute to and lead as required in architectural design, review and engineering of these new services. Perform proof of concept or prototype as necessary upon approval by Government leads.

2B 3.4.3 Sub-objective: Container Microservices (MCaaS)

The Multi-tenant Containers as a Service (MCaaS) is a modern, cloud-native solution leveraging modern container technology based on Kubernetes and promoting an advanced DevSecOps lifecycle methodology. MCaaS integrates enablement services to ensure tenants are successful in their app planning, onramp, and delivery. Resulting in higher flexibility for tenant applications while adhering to operational requirements and delivering scaling efficiencies

Provide a capability for application teams to deploy applications that support containerized design and require orchestration.

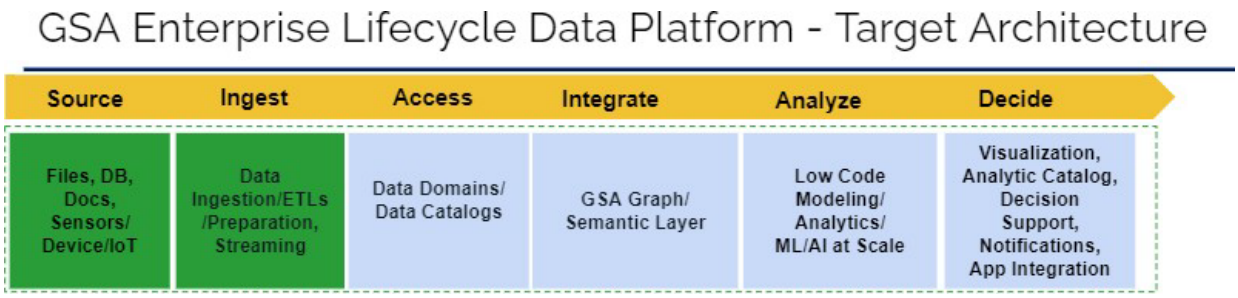
All products, capabilities, or tooling used to support MCaaS shall:

- Be able to support multiple tenants
- Allow application teams to deploy applications without involvement from the service provider
- Allow means for application team to integrate tooling into their build, testing, and deployment process

- Be efficient and develop reusable components to provide automated self-service capabilities to tenants where possible.
- Be re-usable common container or containerization supporting services to promote compact portfolio and streamline application ATO footprint.
- Extensible containerization for various components that provided modularity and
- Define and document service level objectives for the capabilities as well as the components dependent for the service.
- Product metrics aligned with CLOs and integration into the monitoring.
- Maintain customer responsibility information for using the service and how the customer should consume the service.

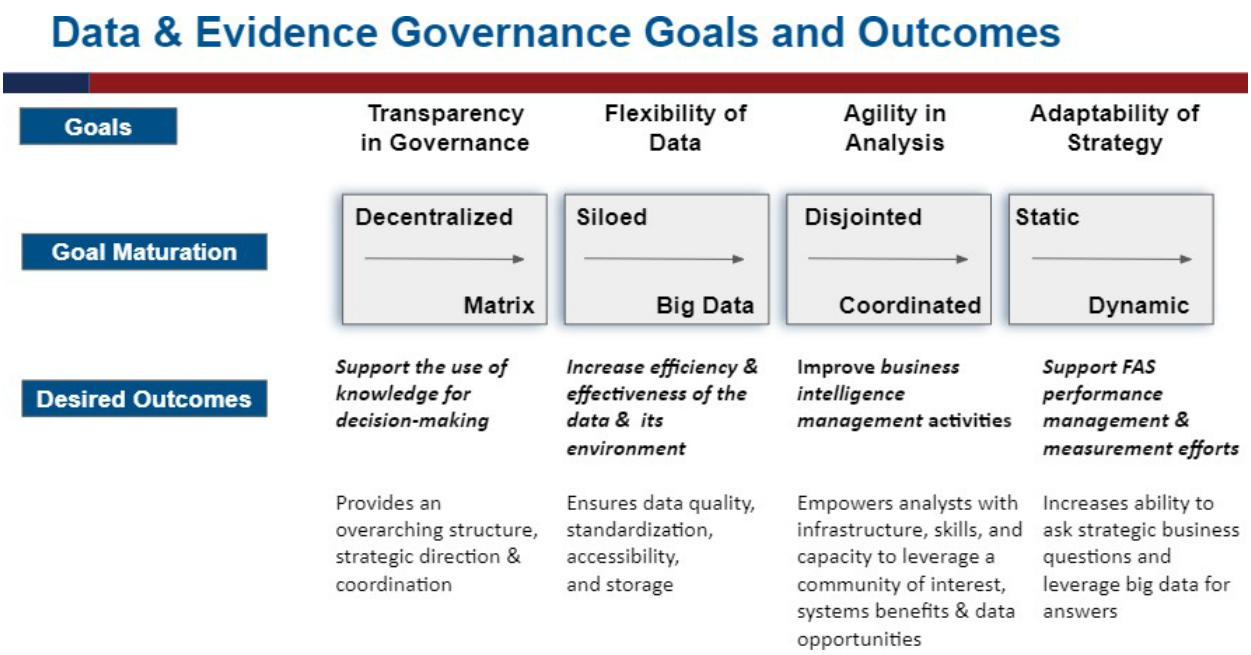
2B 3.4.4 Sub-objective: Data Lifecycle

Data Lifecycle term encompasses all capabilities associated with working with all forms of data. Any of the current services or planned services are in alignment with GSA's Data Lifecycle strategy. GSA IT's Chief Data Officer defined the Enterprise Lifecycle Data Platform Target Architecture. The capabilities for data shall be aligned with the major components.



GSA IT's Enterprise Lifecycle Data Platform - Figure 4.13

Another major governing body which defines the services objectives, maintenance and maturity is the FAS Data & Evidence and Government board.



FAS Data & Evidence Governance Goals - Figure 4.14

A Centralized Data Analytical, Service Wide Coordinated Capability.

To meet these objectives, the contractor shall perform the following:

- Maintain the following services
- Provide recommendations to further enhance services defined in Enterprise Lifecycle Data Platform or FAS Data & Evidence Governance Goals

Data Management
Platform components to manage and track data access control, data custodian roles and responsibilities, data high availability, data storage, data transformation, and notifications (on platform activity related to data management).

To meet this objective, the contractor shall perform the following:

- Manage data dictionary, domain models, and master data management
- Manage the ETL (extract, transform, and load) Services with good data quality.
- Collaboration with business stakeholders on data process and data business logics.
- Establish and maintain the data governance policies, data custodians' roles and responsibilities and as well as the data operation maintenance policy.
- Define and establish the design principles and design patterns for enterprise data model, data lake, and data transformation/ETL. (reference and contribute to GSA IT Playbook)

- Design, implement, and maintain the enterprise data model to fully support the FAS domain data model, the master data management and as well as support data provision and analytics services
- Collaboration with business stakeholders on data onboarding workflow processes, identify and implement data business logics.
- Design, implement and maintain the data lake structure to support the ETL and data analytics service
- Identify and evaluate the new technologies with justification of the cost versus benefit
- Coordinate with FCS teams to build standardized and develop reusable data transformation/ETL services
- Support Future/Existing tenants for Data Encryption with Classified/PII data or per request of the tenant.

Data Governance
A mechanism for the Data and Evidence Governance Board (DEGB) to manage and track: data policy, change management, stewardship roles and responsibilities, data lineage, metadata/dictionary management, data usage, notifications (platform activity related to data governance).

To meet this objective, the contractor shall perform the following:

- Manage FAS Business Activity Catalog
- Demonstrate data flow into FAS Data Model
- Continue to enable the Data Catalog (Alation) features that includes:
    - Alation Analytics V2
    - Alation data lineage
    - New feature releases that enhance the business practice
- Ability to adopt catalog API feature for metadata sharing
- Collaboration with business stakeholders to define and maintain the metadata / data dictionary management process that includes metadata collection, ingestion, and updates.
- Provide the catalog usage dashboard and visualizations of how users interact with the catalog and reveal information on usage intensity and patterns
- Provide maintenance to support change management activities from business and data catalog page updates.
- Provide data catalog user training for data stewards, composers, and viewers

Data Provision
Automated and governed process of provisioning the user requested data access and delivering the JDBC or ODBC endpoint to the requesting user. This service has not been delivered and this is the future state.

To meet this objective, the contractor shall perform the following:

- Collaborate with business stakeholders for requirements gathering and use-case analysis.
- Ability to present the data entities and elements with business definitions / descriptions and support the self-service functionalities where it applies
- Provide and document the scalable and reusable technical solutions to meet business requirements and goals.

Data Delivery
Capability to deliver data models by auto generated data schemas or API to support users' business intelligence (BI) analytics or other applications, and version control between the action and development model. This service has not been delivered and this is the future state.

To meet this objective, the contractor shall perform the following:

- Conduct and document the business use-cases analysis, provide the scalable and reusable technical solutions to meet business requirements and goals.
- Provide the scalable solution to deliver the semantic data in various methods to support BI analytics, and application data consumption
- Incorporate with other FCS common components for a solution to support the self-service functionalities where it applies

Data Analytics/Compute
Managed BI and visualization environments enabling analysts and data scientists to analyze data. Managed big data platform enabling data scientists and data engineers to develop, visualize, and debug data engineering and data science processes at large scale.

To meet this objective, the contractor shall perform the following:

- Maintain and enhance the existing Data Analytics Service and provide the environment and tools necessary for advanced data analytics, AI and machine learning for business data teams to achieve critical business line goals faster, more reliably, and at scale.
- Provide clear coordination with dependent services on maintaining operation
- Manage FAS Business Activity Catalog
- Demonstrate data flow into FAS Data Model

2B.4 Objective: As-Needed Support Objectives

Due to the nature of "Unpredictable" Government changes and initiatives that frequently affect FCS support, there is a need to have ad-hoc services in which the level of effort and anomalies that cannot be anticipated.

When As-Needed Support Objectives are exercised by the Government the contractor will be notified followed by the delivery of revised requirements. The contractor is expected to respond within 10 business days with a written proposal, a cost proposal, and a Staffing Plan for Government review and potential Government/contractor negotiation as needed. On

acceptance by the Government, the contractor will have 20 business days to secure personnel that meet the requirements of the agreed to Staffing Plan, after which the contractor will have 5 business days to submit to the COR personnel security forms in accordance with paragraph **9.5 *Employee Security Requirements*** and **9.5.1 New Contractor Personnel**.

2B 4.1 As-Need Support Sub-objective: Enterprise Infrastructure and Cloud Services Advisory

Cloud Advisement & Enablement shall expand when a significant amount of strategies is required for the agency. This will be expanding the requirements from Objective 2: Labor Services. The contractor shall support the growth in advisory services necessary to provide adequate services for future business system cloud transformations.

2B 4.2 As-Need Support Sub-objective: Data and Evidence Governance Board (DEGB) Advisory

This role shall support the efforts of the FAS Enterprise Data Architecture and how to further mature the organization's data management policies. This role must be able to align to the FAS Enterprise Data Architecture requirement on adopting and using services to meet FAS's mission of "A Centralized Data Analytical, Service Wide Coordinated Capability'. This role must evaluate the current state and the governance framework and make determines on how to increase effective adoption and provided enterprise level Data Governance Framework maturity as follows:

To meet this objective, the contractor shall perform the following:

- Support the Data Owners and Data Stewards in following Data Governance processes it aligns with the domain concepts the DEGB has defined.
- Expand the Domain Owners and Data Stewards' roles or responsibilities in a matter to scale the program for all of the Acquisition life cycle.
- Preparation and administration for Data Governance Committee meetings.
- Coordinate and support a business glossary and leverage the Data Governance Services to capture this information.
- Support the establishment and management of the Data Quality Issue Management process.
- Support the maturity for the domain change control processes and operate within the Data Management Service.
- Establishing the measures to evaluate the effectiveness of these governance frameworks on improving the organization's adoption and providing more value to execute the mission must be done on a routine evaluation.
- Establishing the communication strategy on how this program can support senior leaders and all members requiring data. Including by not limited to facilitating a data submit, holding domain steward working sessions or facilitating any type of engagements with the stakeholder to gain adoption on the data strategy.

2B 4.3 As-Need Support Sub-objective: Major Business system modernization

This is a placeholder for cloud support work that would be related to a future modernization effort that does not fit into the service model. Any labor would align with Objective 2 or Objective 3 of this PWS. The government recognizes that all business system transformations are not the same size nor complexity. It is anticipated that there will be varying sizes and complexity requiring support and the contractor shall support the execution of these future business system cloud transformations.

2B 4.4 As-Need Support Sub-objective: Semi/Fully-managed Services Growth

It is vital that the EcoSystem continues to provide more services for the tenants. This requires following the Cloud Advisory and Cloud Engagement Process. All services/technologies shall apply the following Subtask 3.1: Software Development and Coding Practices, Subtask 3.2: DevSecOps Framework and Subtask 3.3: Building Cloud Native.

2B 4.4.1 As-Need Support Sub-objective: Function Microservice Services

FAS Cloud Services, (FCS), announced that Serverless Framework-as-a-Service (SFaaS) would be generally available for the application development teams. SFaaS is an FCS service enabling application teams to develop, deploy, monitor and secure serverless applications within the FCS EcoSystem.

SFaaS allows the application team to focus their efforts on what provides value to their customers, not wasting time on infrastructure as code, scaling and maintaining any infrastructure. SFaaS provides consistent developer experience of infrastructure provisioning, application deployment and monitoring, alerting, logging and troubleshooting for serverless applications.

To meet this objective, the contractor shall perform the following:

a. Stick to shift security to the left design principle and collaborate with GSA Security as required throughout all phases of service development lifecycle.
b. Consult with industry experts and propose, recommend and implement industry best practices and design principles.
c. Contribute to, assist and/or lead design of SFaaS service and develop capabilities including but not limited to serverless compute, database, messaging, notification, streaming, workflow management and orchestration, opentracing and supporting various application architectures including but not limited to API-driven, Event-driven and data streaming.
d. Automate infrastructure as code to ensure consistent, repeatable provisioning, update, versioning, deployment, upgrade, scaling and termination of the SFaaS service. Leveraging reusable infrastructure shared service components and modules as much as possible.
e. Seamlessly Integrate with existing FCS products and services, including but not limited to FCS source code repository, artifact repository, FCS IDM, FCS freedom pipeline, FCS AIR, FCS Data Services, FCS EBTA, MCaaS and Monitoring/Logging services.

f. Automate service provisioning and deployment with integrated DevSecOps process and security and compliance testing.
g. Design, implement automation of proper tagging strategy for SFaaS to support multi-tenancy cost model and reporting.
h. Automate tenant onboarding process to the maximum for SFaaS service.

2B 4.4.2 As-Need Support Sub-objective: CI / CD Services

The CI/CD Pipeline - Provides application teams a pre-built development process with securely configured components to further support modern software development patterns. The government believes that many aspects (85%+) of the security requirements are inherent within the services and environment where the applications reside.

In support of this subtask the contractor shall:

- Identify and present opportunities for standardization, modernization, product enhancements, cost reduction, and adoption on a quarterly basis.
- Provide tenant consumable CI/CD services that allows tenants to define how to use the service within their operating environment, automation and tenant maturity, software testing, and other development related topics as directed by the government on a quarterly basis.
- Provide technical guidance and assistance to CI/CD platform consumers as required by the government.

2B 4.4.3 As-Need Support Sub-objective: Code Management Services

The Code Management platform is leveraged by all projects and services within the Cloud Services. This provides our tenants with a version-controlled code repository where they can manage their application code, Infrastructure as Code, security as code, configuration management code, and change management process.

In support of this subtask the contractor shall:

- Identify and present opportunities for standardization, modernization, product enhancements, cost reduction, and adoption of DevSecOps, Infrastructure as Code, cloud services, and software development on a quarterly basis.
- Create guides/playbooks for common toolchains, languages, patterns, software testing, frameworks and processes used by the government to assist teams in adoption and maturation.
- Monitor and report on common code practices, automation and tenant maturity, software testing, and other development related topics as directed by the government on a quarterly basis.
- Provide operational support, maintenance, patching, and continuous improvement for the code repository platform.
- Provide training, marketing, and evangelist support to ensure customers are aware of current and upcoming features and can understand and leverage the Code Management platform.
- Provide technical guidance and assistance to consumers of the Code Management platform as required by the government.

2B 4.4.4 As-Need Support Sub-objective: Artifact Management Services

The Artifact Management platform is leveraged by all projects and services providing them with the ability to download the latest versions of dependencies, application builds and is an integral part of our supply chain risk management strategy.

In support of this subtask the contractor shall:

- Identify and present opportunities for standardization, modernization, product enhancements, cost reduction, and risk reduction relating to Artifact management, code signing, package management, artifact management, and release management on a quarterly basis.
- Create guides/playbooks for common code signing, artifact management, package management, and release management processes and procedures to assist teams in adoption and maturation.
- Monitor and report on common supply chain risk management practices, tenant maturity, and other package, artifact, and release management topics as directed by the government on a quarterly basis.
- Provide operational support, maintenance, patching, and continuous improvement for the code repository platform.
- Provide training, marketing, and evangelist support to ensure customers are aware of current and upcoming features and can understand and leverage the Artifact Management platform.

2B 4.4.5 As-Need Support Sub-objective: Image Management Services

The Image Management platform delivers an operating system and container image pipeline for providing updated and hardened images available to product teams.

In support of this subtask the contractor shall:

- Identify and present opportunities for standardization, modernization, product enhancements, cost reduction, and risk reduction relating to operating system image creation and container image creation on a quarterly basis.
- Create guides/playbooks for Image Management processes and procedures to assist teams in adoption and maturation.
- Monitor and report on common image management topics as directed by the government on a quarterly basis.
- Provide operational support, maintenance, patching, and continuous improvement for the code repository platform.
- Provide training, marketing, and evangelist support to ensure customers are aware of current and upcoming features and are able to understand and leverage the Image Management platform.

2B 4.4.6 As-Need Support Sub-objective: Log and Event Management Services

Monitoring and Alerting: FCS uses a Collaborative Roadmapping approach to enhance the FCS-wide monitoring solution. The Log and Event Management solution will provide the functionality and data necessary to measure, monitor, and alert on system performance and SLA/SLO metrics and thresholds across all FCS infrastructure.

In support of this subtask, the contractor shall:

- Automate using infrastructure as code as stated in Building Cloud Native Objective
- Manage and maintain a centralized logging and monitoring solution to streamline maintenance and root cause analysis for all IT stakeholders.
- Automate onboarding of new tenants to the shared services logging system to ensure consistent, repeatable environments and procedures
- Create tenant alerts to notify tenants when they are close to reaching their limits
- Follow the program-wide instrumentation standards to enable usage-based cost recovery and/or showback
- Perform and support any migration or convergence efforts to new products
- Create and deliver technical SOPs for any new FCS monitoring and alerting services

3. QUALITY

Both the Contractor and the Government have responsibilities for providing and ensuring quality services, respectively.

3.1 Contractor Quality Management

The contractor shall identify and implement its approach for providing and ensuring quality throughout its solution to meet the requirements of the PWS via the contractor's Quality Management Plan (QMP). The QMP shall describe the application of the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing performance requirements. The QMP shall describe how the appropriate methodology integrates with the Government's requirements. The contractor shall make the QMP available to the Government for review upon request and shall obtain acceptance of the QMP by the CO as required. The contractor shall make appropriate modifications to the QMP (at no additional cost to the Government). The Government has the right to require revisions of the QMP (at no cost to the Government) should the QMP fail to deliver the quality of the services required at any time during performance.

3.2 Performance Based Requirements – Performance Measures

This contract / order includes specific performance measures in Attachment 1, Tab H. The performance measures augment the QASP (Quality Assurance Surveillance Plan) by providing performance targets and acceptable levels of product or service quality for specific deliverables that are more detailed than the performance expectations described in the QASP. The performance measures define Acceptable Quality Levels (AQLs) in conjunctions with the evaluation of contractor performance.

3.3 Government Quality Assurance Surveillance Plan (QASP)

The Government will periodically evaluate Contractor performance under this contract / order in accordance with the attached Quality Assurance Surveillance Plan (QASP). The purpose of this evaluation is to ensure that Contractor performance meets Government requirements. The Government reserves the unilateral right to change the QASP at any time during contract performance provided the changes are communicated to the Contractor by the effective date of the change. The QASP along with the included "Surveillance Objectives, Measures, and Expectations" describes the evaluation procedures, PWS items to be evaluated, and the measures against which performance will be evaluated. The Government reserves the right to review services to be provided, including those developed or performed at the contractor's facilities, to determine conformity with performance and technical requirements as prescribed in the applicable inspection clause (see Paragraph 9.14, below). The evaluation results will be documented in the Contractor's CPARS (Contractor Performance Assessment Reporting System) report. The QASP is provided as an attachment to this PWS – **(See Attachment B)**.

4. DELIVERABLES

4.1 Contractor Submission

Support services shall be performed to meet a specific task objective. In some cases, the task objectives and the period of performance shall be stated on individual Task Directives (See Paragraph 9.9, below). Support services and data items shall be delivered to the Government in compliance with the performance measures and quality requirements set forth in the QASP. (Quality Assurance Surveillance Plan, See **Attachment 2**)

Deliverables are to be transmitted with a cover letter on the prime contractor's letterhead. Each deliverable shall include an introductory summary describing the contents.Deliverables shall be provided electronically through GSA's web-based procurement system,as required, and to any other destination(s) as required per the Government's request. The contractor shall provide hard copy deliverables as required per the Government's request. All deliverables shall be produced using software tools/versions as approved by the Government.

All deliverables developed are the property of the Government and must not be used by the Contractor for any other purpose. All project-related information or documentation, with no exceptions, must be treated as confidential and proprietary during and after the completion of this effort and submitted to the project lead. Additional supplemental restrictions or qualifications or acceptance criteria may be provided by the COR through a written technical directive

4.2 Government Review

Government personnel will have ~~10~~ 7 business days to review deliverables (to include resubmissions) and provide written acceptance/rejection. Authorized Government representatives will notify the contractor of deliverable acceptance or provide comments in writing. The contractor shall incorporate Government comments or provide rationale for not doing so within 5 business days of receipt of comments. Government acceptance of the final deliverable will be based on resolution of Government comments or acceptance of rationale for non-inclusion. Additional changes volunteered by the contractor will be considered a

resubmission of the deliverable.

4.3 Government Delays in Reviewing Deliverables or Furnishing Items

If contractor performance or submission of deliverables is contingent upon receipt of government furnished items (data, equipment, materials, facilities, and support) or input, or upon government review and approval of interim items or draft documents (collectively referred to as Government Performance), the government shall specify when it will provide such items or input, or the time it will need to perform reviews or give approvals. If the government fails to meet item, input, review, or approval deadlines, contractor performance or submission of deliverables shall automatically be extended one calendar day for each day of government delay. The contractor shall promptly advise the Contracting Officer of any delays in receipt of government furnished items, input, reviews, or approvals. If dates for Government performance are not specified in this contract/order or associated task directives, this clause will not apply, and contractor delays must be handled or negotiated under other provisions of this contract or order.

4.4 Deliverable Table

The contractor shall perform or deliver the items listed in the following table on the dates and to the locations specified.

PWS Ref.	Event or Item Title	Delivery Time	Delivery Place
	Project Start	Date of Award	
Paragraph 8.1	Contractor Employee Non-disclosure Agreement (one for each employee assigned to work on this order	After award but prior to commencement of performance by each Contractor or Subcontractor employee	Electronically to the GSA ASSIST System & email to the CO and the COR
Para. 2A.2.1	Kick-off Meeting	within 5 business days after award or as agreed by the parties	
Para. 2A.2.1	Kick-off Meeting Minutes	within 5 business days after the kick-off meeting	Electronically to the GSA ASSIST System & email to the COR
Para 2B 1.1.2	Program Management Plan - Draft	within 5 business days after the kick-off meeting	Electronically to the GSA ASSIST System & email to the COR
Para 2B 1.1.2	Program Management Plan - Final	within 5 business days after Gov acceptance of final Draft.	Electronically to the GSA ASSIST System & email to the COR
Para 2B 1.1.2	Program Management Plan – updates	within 5 business days after notifying the Government.	Electronically to the GSA ASSIST System & email to the COR
2B1.3	Incident Response Plan	within 10 business days after the kick-off meeting	Electronically to the GSA ASSIST System & email to the COR

2B1.3	Configuration Management Plan	within 10 business days after the kick-off meeting	Electronically to the GSA ASSIST System & email to the COR
Para 2B 1.1.2 & 2B1.4	Stakeholder Management Plan	within 10 business days after the kick-off meeting	Electronically to the GSA ASSIST System & email to the COR
2B1.5	Risk Management Plan	within 10 business days after the kick-off meeting	Electronically to the GSA ASSIST System & email to the COR
Para. 3.1	Quality Management Plan-Draft	10 Business Days after award	Electronically to the GSA ASSIST System & email to the COR
Para. 3.1	Quality Management Plan-Final	30 Business Days after Government review. (The Government shall review and provide comments within 7 business days after receipt of the draft QCP.)	Electronically to the GSA ASSIST System & email to the COR
Para. 4.5.9	Phase-in Plan - Draft	Delivered at the kick-off meeting	Email to the COR
Para. 4.5.9	Phase-in Plan - Final		Email to the COR
Para. 5.3.1	Emergency Off-Hours Support Model	30 Business Days after Kick-off meeting	Electronically to the GSA ASSIST System & email to the COR
Para. 4.5.4	Staff Matrix A complete and current list of Contractor employees and the task/office/function they are supporting	Furnished at the kick-off meeting with an update furnished on or before the date of any personnel change.	Electronically to the GSA ASSIST System & email to the COR
Para. 4.5.5	Funds and Expenditure Report	No later than (NLT) 5 business days after the end of the month	Electronically to the GSA ASSIST System & email to the COR
Para. 4.5.6	Monthly Status Report – Final	NLT 15th day of the month.	Electronically to the GSA ASSIST System & email to the COR
Para. 4.5.7	Technical Reports Studies - Draft	As required	Email to the COR

Para. 4.5.7	Technical Reports Studies - Final	10 Business Days after Government review. (The Government shall review and provide comments within 7 business days after receipt of the draft report/study.)	Email to the COR

4.5 Data Requirements / Descriptions

Documentation provided in response to the objectives will be in the Government's template format. If no format is prescribed, documents may be in the Contractor's preferred format using Google G Suite products.

The content of all data items, if not self-explanatory from the template format, shall be agreed upon between the parties.

4.5.1 Contractor Employee Non-Disclosure Agreement

The Contractor shall furnish a signed "Contractor Employee Non-Disclosure Agreement" for each Contractor and Subcontractor employee assigned to work under this contract / order, prior to their starting work.

4.5.2 Kick-off Meeting Minutes

The Contractor shall take minutes of the kick-off meeting which shall captures the the names of the attendees, the key points of the discussion, questions raised and answered, and action items.

4.5.3 Quality Management Plan

The Contractor shall deliver a QMP as defined in Paragraph 3.1, above.

4.5.4 Staff Matrix

The Contractor shall furnish a complete and current list of Contractor and Subcontractor employees who are assigned to work under this contract / order. The matrix shall include the staffing chart showing the name of each employee, his or her position in the staffing plan, job title, and the Government's task/office/function they are supporting.

The lines of authority and responsibility of each staff member shall also be made clear to the Government. The matrix shall be updated with each change in personnel, job title, position in the staffing plan, or assignment of area of responsibility.

4.5.5 Funds and Expenditure Report

The contractor shall provide a Funds and Expenditure Report that provides the current task order accounting information indicated below in support of the monthly invoice. The Contractor can determine the format of the report provided it includes, at a minimum, the following information:

- Expenditures for labor, material, travel, and any other charges.
- Matrix of Actual hours expended vs. planned and/or funded hours, and an explanation of significant variances between planned and expended hours. The report shall include amounts for the current monthly reporting period and the cumulative actual vs. planned hours and amounts for the entire contract/order up to the report date.
- Burn rates for the current period and the cumulative amount for the entire contract/order up to the report date. The information shall be presented in numerical and chart format for each CLIN
- Cross-walk of costs incurred for work performed to amounts billed.
- Current and cumulative task funding status (direct labor, travel, and other direct cost funding status to be reported separately, if required).
- Charges for Support Items, which are authorized in the task (e.g., travel, training, etc.).

Charges shall not exceed the authorized cost limits established for labor and support Items. The government will not pay any unauthorized charges. Original or copies of receipts, travel vouchers, etc. shall be maintained by the contractor to support charges other than labor hours and made available to government auditors upon request. Travel documents shall be furnished in accordance with government Travel Regulations

4.5.6 Monthly Status Report (MSR)

The contractor shall provide a MSR that briefly summarizes, by task, the management and technical work conducted during the month. The contractor shall provide the following information, plus any other information that the contractor determines to be germane to the tasks.

- Status of tasks, schedules, deliverables summarizing the effort and progress of all activities. Status of tasks shall include a summary description and updated milestone schedule noting changes, issues and/or variances, concerning --

- all tasks completed and their related deliverables submitted during the reporting period. The relationship of deliverables to the milestone schedule shall be shown,
- all tasks currently on-going during the reporting period, and
- all known tasks assigned and activities planned for future reporting periods, and
- all standards that are being followed in support of the requirements.
  - New work added since the previous Monthly Status Meeting
  - Problems or issues and proposed resolutions
  - Government action requested or required

4.5.7 Technical Reports

Content and format of technical reports shall be agreed upon between the parties.

4.5.8 Trip Reports (not applicable)

4.5.9 Phase-In Plan

Transition occurs at two key points during the period of performance: 1. task order award and 2. task order end/conclusion. At task order award, a transition must be accomplished as the Contractor (if not the incumbent) transitions from the incumbent Contractor (Transition-in). At task order/contract conclusion, the Contractor must transition to the new Contractor (Transition-out) if not selected for follow-on work.

The Phase-In transition period is defined as the period of time when the new contractor and the incumbent contractor will both be providing support to the client as required to support the transition to the newly awarded contract/order.

During the task order kick-off meeting, the contractor shall present the Phase-In Plan that was submitted in response to the task order solicitation. As noted in the solicitation, the Phase-In Plan shall present a clear understanding of the phase-in tasks required, the issues likely to result from non-incumbent contractor performance, and the contractor's proposal to resolve such issues. The phase-in plan shall include a clear and feasible strategy for delivering services required within the periods specified by the plan and shall include a detailed plan-of-action and milestones to transition the functions identified in this PWS in a well-planned, orderly, and efficient manner. The phase-in plan shall include, at a minimum:

- Development and submission of required deliverables.
- Interface with the Government and incumbent contractor (if applicable) during phase-in, to include meetings or status reports, as required.
- Approach to maintaining quality and minimizing disruption during phase-in.
- Development and dissemination of operating instructions, procedures, and control directives.

Specific to this task order, during the transition in, the contractor shall ensure that there will be minimal service disruption to GSA applications, no service interruptions to mission critical systems as identified in Attachment 1, Tab H, and no service degradation during and after transition using existing tools and processes in place. All transition activities shall be completed no later than 90 calendar days after contract award; individual systems and applications may be transitioned using a staged approach. The transition in plan shall include an Operational Readiness Review (ORR) that outlines the contractor's preparedness to assume operation of TO duties for each of the 50 applications. The Contractor shall assume application responsibilities and management of the systems after conducting a meeting demonstrating Operational Readiness. Written Government approval will be granted upon successful outcome of the meeting.

The contractor shall provide daily status updates to the GSA application owners, and a weekly Transition Status Report. On an application level, this report shall detail:

1. The application transition phase, as identified in the contractor's Transition Plan.
2. Performance against the contractor's application transition schedule.
3. Status of any in-flight or in-progress projects.
4. The contractor's staffing status, to include security processing.
5. The contractor's applications acceptance plan, checklist, schedule, and process.
6. Transition risk management and mitigation.
7. Coordination and activities with the previous application management contractor.

4.5.10 Phase-Out Plan

Should it be necessary to transition the work performed under this task order to another vendor, the Contracting Officer may notify the contractor to prepare and implement a Phase-Out Plan. If such notification is given, the following requirements will apply.

During phase-out of the contract/order, which is determined to be a period of 60 calendar days prior to the lifecycle end date of the contract/order, a smooth and orderly transition between the incumbent contractor and the successor contractor is necessary to ensure a minimum disruption to vital Government business. The contractor shall cooperate to the extent required to permit an orderly changeover to the successor contractor. The phase-out will be deemed completed by the COR and/or other identified Government representatives when it is determined by the Government that the transition of property, data, and information developed as a part of the contract/order have been successfully changed over from the outgoing contractor to the Government and the successor contractor as required. Phase-out activities include, but are not limited to, the tasks below.

- Submission of official comprehensive phase-out plan.
- Daily communication of staffing status (i.e. projection of when incumbent contractor employees will off-board from the incumbent contract/order and identification of additional incumbent resources, such as a transition team, that may be needed to support the transition efforts) and overall phase out status, in accordance with the accepted phase-out plan.
- Maintain the phase out schedule included within the phase-out plan.
- Transition of property.
- Transition of supporting documentation.
- Transition of accounts (e.g. user accounts and user access).
- Knowledge transfer on the established installation, operation, and maintenance procedures of the technologies supported. The phase out plan shall clearly describe the proposed methodologies to be utilized for such transfer (e.g., written documentation, manuals, formal classroom type training, one-on-one training sessions, etc.).
- Execution and submission of phase out checklist, to include Government acceptance.

Specific to this task order, the contractor shall identify how they will coordinate with the incoming Contractor and/or Government personnel to transfer knowledge regarding the following:

1. Project management processes.
2. Points of contact.
3. Location of technical and project management repositories.
4. Status of ongoing technical activities.
5. Appropriate Contractor to Contractor coordination to ensure a seamless transition.
6. Transition of Key Personnel
7. Transition of current work in progress/backlog. Schedules and milestones (e.g., bug releases, minor enhancement releases, security vulnerability remediation)

The Contractor shall also establish and maintain effective communication with the incoming Contractor and Government personnel for the transition period as required, but no less than weekly via the established weekly status meetings.

The Contractor shall implement its Transition-Out Plan, per Government approval, no later than 60 days before the expiration of the task order.

4.5.11 Monthly Invoice

The contractor shall provide a monthly invoice, no later than the 15th calendar day of the month following the monthly reporting period, to be submitted simultaneously with the MSR. As applicable, the invoice shall include but is not limited to:

- Clear identification of all costs.
- Labor hours expended (for labor hours tasks). The labor hours expenditure information shall include the identification of the employee name, labor category, hourly labor rate, and total number of labor hours expended.
- Timecards. As required, the contractor shall provide a copy of each employee's timecard/sheet. The timesheet shall identify the contractor employee name and number of hours claimed per day.
- Travel costs.
- Supporting documentation for travel costs. Refer to PWS 5.3 for specific requirements.
- Other Direct Costs.
- Supporting documentation for other direct costs. Refer to PWS 9.6 for specific requirements.

As required, the contractor shall comply with line item (i.e., per individual positions, different programs, program areas, etc.) invoicing requests

4.5.12 Other Reports

Content of other reports is self-explanatory or should be agreed upon between the parties.

5. PERFORMANCE PLACE, TIME, AND RESTRICTIONS

5.1 Period of Performance

The anticipated period of performance(s) is/are identified below. The Government reserves the unilateral right to exercise an option period prior to the expiration of the Base or option period

- Base Period: Initial 12 months from date of award
- Option Period 1: 12 months following the Base Period
- Option Period 2: 12 months following Option Period 1
- Option Period 3: 12 months following Option Period 2
- Option Period 4: 12 months following Option Period 3

5.2 Place of Performance

5.2.1 Performance at the Contractor's Facility

Work is expected to be performed primarily at the contractor's facilities. Work performed at contractor facilities shall be performed according to the contractor's standard commercial practice; however, the contractor representatives at these facilities must be available for interaction with Government employees during the core hours identified in

the paragraph entitled “Time of Performance - Normal Hours”, below, with the exception of Government designated holidays or facility closures.

On occasion, placing contract personnel in Government facilities may be necessary for efficient execution of a task or support in person meetings as required. At least one business day of notice will normally be provided.

5.2.2 Performance at the Government’s Facility

The Contractor may be required to perform work at GSA headquarters to attend meetings, enable the Contractor to work with GSA to understand the business needs and provide continuous delivery of functionality, conduct training sessions, troubleshoot, etc. Only local, non-reimbursable travel is anticipated

5.2.3 Applicability of Telework

All work performed at locations other than those identified as Government and/or contractor facilities shall be approved prior to performing the work. Federal contractors are not governed by Office of Personnel Management (OPM), GSA, or the individual agency policies; however, this does not prohibit contractor personnel from actuallyworking at an alternate site, when/as appropriate and specifically authorized by the Government. The contractor shall develop telework policies to comply with the followingrequirements and address such requirements at a generic level within their QMP. Alternate work arrangements for contractors shall be negotiated with the contractor’s ownemployer and the appropriate agency official, to ensure policies and procedures are in close alignment and there is a clear and concise arrangement documenting the agreement. It remains the contractor’s responsibility to ensure the services are performedin accordance with the terms and conditions of the contract/order.

The contractor shall address the pertinent facts impacting performance and ensure all affected contractor resumes and other related documentation reflects the applicable work site. The contractor shall provide justification to the Government when identifying and submitting an individual as a telecommuter and address implementation processes and procedures within the QMP. The contractor shall be responsible for ensuring the Government has the required access/details necessary for the Government to perform quality assurance responsibilities.

The contractor shall comply with all agency security telework policies. The contractor shall ensure all services provided from an alternate site comply with the Federal Information Security Management Act of 2002 (FISMA) and address the following, as a minimum:

- Controlling access to agency information and information systems;
- Protecting agency information (including personally identifiable information) and information systems;
- Limiting the introduction of vulnerabilities;
- Protecting information systems not under the control of the agency that are used for teleworking;
- Safeguarding wireless and other telecommunications capabilities that are used for teleworking; and
- Preventing inappropriate use of official time or resources that violates

subpart G of the Standards of Ethical Conduct for Employees of the Executive Branch by viewing, downloading, or exchanging pornography, including child pornography.

5.2.4 Unplanned Government Facility Closures

In the event of unplanned closure of the Government facility for any reason (e.g. natural disasters, Government shut-down, or severe weather) the Contractor shall make its best effort to mitigate loss of work time. If Contractor employees are working on the Government facility, this may be done by moving employees to an off-site location. If performance under this contract/order is not possible, the Contractor shall take steps to assign employees to other projects on a temporary basis or place them in leave status to minimize non-productive costs to the Government under this contract/order. Additional instructions may be provided by the Contracting Officer on a case-by-case basis. Disagreements between the parties resulting from closures shall be settled through negotiations to the maximum extent possible or shall otherwise be settled pursuant to the provisions of the Disputes provisions of this contract/order.

All services to be performed under this contract/order have been determined to be non-essential for performance during a closure. Should the Government facility be closed, the Contractor shall be notified by either the Contracting Officer, COR, or a local television or radio station. The Contractor is responsible for notifying its employees about Government closures. Contractor employees are not to report to the Government facility if it is closed and will adhere to delays, unless otherwise specifically instructed otherwise by the CO or COR.

5.3 Time of Performance - Hours of Work

5.3.1 Normal Hours

For any Contractor employees working on Government facilities normal business hours are between 7 AM – 5 PM Eastern time, Monday through Friday, with core hours 9 AM - 3PM., excluding holidays, to coordinate with Government operations. Actual start and end times shall be at the contractor's discretion. The Contactor shall be responsible for managing the work hours of its employees who work at Contractor facilities, provided that those employees are available when necessary, to interact with Government employees (normally between 8 AM and 5 PM Eastern time).

Any Contractor employee working at Government facilities shall observe federal holidays and government closures on the same dates and during the same times as the Government personnel, since Contractor employees shall not have access to the Government facilities during these days and/or times. These holidays are as follows.

Off Hours
The contractor shall develop, scope and implement a sustainable Off Business Hours support model, with a strategy for providing emergency off-hours support. For Contractor employees working or meeting in Government facilities, after business hours support are as agreed to with the government COR.

If Contractor employees are working at Government facilities and task completion deadlines require extended hours, the Government will provide authorization to occupy and use Government facilities beyond normal duty hours.

5.3.1 Holidays

The Government shall observe the following holidays.

New Year's Day	Labor Day
Martin Luther King Jr., Day	Columbus Day
Presidents' Day	Veteran's Day
Memorial Day	Thanksgiving Day
Juneteenth	Christmas Day
Independence Day	

5.3.1 Expedited Performance

In the event that individual tasks or subtasks require expedited performance or extended workdays to meet schedule constraints or work volume, the Government shall communicate that need to the Contractor's Project Manager or Team Lead who, in turn, is responsible for managing the Contractor's labor resources to meet the schedule constraints. Communications regarding expedited performance shall be documented in writing, by email or otherwise, and included in the contract administration file. If Contractor employees are working at Government facilities and task completion deadlines require extended hours, the Government will provide authorization to occupy and use Government facilities beyond normal duty hours.

5.4 Travel (not applicable)

5.5 Limitations on Contractor Performance

In compliance with FAR 37.102(c), this task order does not require the contractor to perform any inherently governmental functions. Accordingly, the contractor shall NOT perform any of the inherently governmental functions listed in FAR 7.503. Those inherently governmental functions most applicable to this procurement action are as follows:

- Determine Government policy. [7.503(c)(5)]
- Determine Federal program priorities. [7.503(c)(6)]
- Direct or control Federal employees; [7.503(c)(7)]
- Determine acquisition, disposition, or disposal of Government property; [7.503(c)(11)]
- Determining what supplies or services are to be acquired by the Government [7.503(c)(12)(i)]
- Vote on a source selection board; [7.503(c)(12)(ii)]
- Approve any contractual document on behalf of the Government; [7.503(c)(12)(iii)]
- Award Government contracts; [7.503(c)(12)(iv)]
- Administer Government contracts; [7.503(c)(12)(v)]
- Accept or reject supplies or services; [7.503(c)(12)(v)]
- Terminate Government contracts; [7.503(c)(12)(vi)]
- Determine cost reasonableness, allowability, or allocability; [7.503(c)(12)(vii)]
- Participating as a voting member on performance evaluation boards; [7.503(c)(12)(viii)]
- Determine budget policy, guidance, and strategy [7.503(c)(16)]

6. PERSONNEL

6.1 General Requirements

%%%

NOTE: The Government, at its sole discretion, may consider substitutions and/or requests for deviation from any of the following personnel qualifications (e.g., experience in lieu of education), if to do so would be in the best interest of the Government.

%%%

All contractor personnel shall meet the minimum general requirements listed below.

- All personnel shall be capable of working independently.
- All personnel shall have training and experience that is appropriate for the tasks to which they will be assigned.
- The contractor shall provide personnel that are capable of conducting themselves in a professional manner and have proper telephone and e-mail etiquette, customer service techniques, and organizational skills.
- Contractor personnel performing in a leadership capacity shall be capable of directing contractor personnel and interfacing with the Government and customers.
- Ability to communicate applicable technical subject matter expertise to management and others.
- Strong written and oral communication skills in the English language. All contractor personnel must be able to read, write, speak and understand English.
- Exceptional customer service skills.
- Strong time-management and prioritization skills.
- If applicable, all personnel shall meet the minimum requirements set for in the Federal Supply Schedule (FSS) contract or Government-wide Acquisition Contract (GWAC) upon which this task order is based.

The Contractor shall furnish adequate documentation to substantiate compliance with this requirement for each assigned staff member. The Contractor shall certify as to the accuracy and completeness of the supporting documentation.

6.2 Specific Expertise and Experience

The contractor shall provide personnel with the appropriate skill levels. While each individual contractor employee may not possess expertise and experience in each area of performance, the Government requires that the overall contractor staff possess the aggregate skills, expertise, and experience to successfully complete all requirements and each of the tasks in this PWS. Specific expertise and experience requirements of Key Personnel is provided in Paragraph 6.4.1, below.

6.3 Training

6.3.1 Contractor Staff Training

The contractor shall provide fully trained and experienced staff. Contractor personnel are required to possess the skills necessary to support the minimum requirements of the labor category under which they are performing. Training of contractor personnel shall be performed at the contractor's expense, except when the Government changes the requirements during performance of an on-going task and it is determined to be in the best interest of the Government. This will be negotiated on a case-by-case basis. Training at Government expense will not be authorized for replacement personnel or for the purpose of keeping contractor personnel abreast of advances in the state-of-the-art, or for training contractor personnel on equipment, computer languages, and computer operating systems that are available in the commercial market.

> ***NOTE: Unless Contractor employee training is specifically identified and authorized by the Government, in writing, the Contractor shall not bill the Government for employee time spent in training or for any costs related to or associated with Contractor employee acquired training. This applies to training of any type or for any purpose, including training that is either necessary for job or employment eligibility or a prerequisite to performance of work under this contract/order, whether general in nature or specialized and unique to this requirement.***

6.3.2 Mandatory Government Training

During the course of this contract / order the Government may require Contractor employees to receive specialized training in areas necessary to allow the Contractor to fulfill the requirements of this contract / order (e.g., LAN Information Assurance Training, Government unique software or software tools, Security Training). In such cases Government mandated training shall be considered part of this contract and charged against the task(s) to which the individual Contractor employee is assigned.

Mandatory Government training shall be tracked and monitored by the contractor. All required courses must be completed by the required dates by all contractor personnel. Mandatory Government training classes may be completed during work hours. It is the intent of the Government to provide 30 calendar days written notice of annual training requirements to the designated contractor representative. The designated contractor representative will be responsible for notifying subordinate contractor personnel. Failureof Contractor employees to take mandatory Government training may impair the Contractor’s ability to perform but will not excuse the Contractor from performing.

6.4 Key Positions / Key Personnel

6.4.1 Definition & List of Key Personnel

Key Personnel are defined as those individuals who are so essential to the work being performed that the contractor shall not divert them to other projects or replaced them without receiving prior approval from the Contracting Officer. This includes substitution of those originally proposed at the time of contract/task order award.* Substituted personnel must have equal or better qualifications than the person they replace, subject to the Government’s discretion. Additionally, all key personnel assigned to this task ordershall be dedicated to this project to the extent that they contribute their time equal to oneFTE (full time equivalent) per task order period of performance equally distributed

throughout the year. For this task order 1 FTE = 1920 labor hours.

The following positions along with their requirements are those that the Contractor is to fill with "Key Personnel" under this task .** The Government has identified 5 "Key Personnel" that are intended to be filled upon award as Mandatory, as shown below. Refer to **Attachment A, Tab A** for a listing of those positions that the Government has designated as "Mandatory". The personnel positions listed below as "Optional" are not initially designated as Key Personnel but may be added as "Mandatory Key Personnel" at the discretion of the Government at some point during the life of the task order. Contractor employees who fill any "Mandatory" positions must be listed as Key Personnel by name. The Government does not intend to dictate the composition of the ideal team to perform this task order. Therefore, the Government will allow and will evaluate up to two additional Key Personnel as proposed by the offeror.

The Government desires that Key Personnel be assigned for the duration of the task order.

> **Note: Failure of the Contractor to furnish proposed key personnel shall be viewed as a breach of contract and may be grounds for a default determination by the Government.*
>
> ***Note: Should the Contractor propose additional key personnel this provision will be modified to include those additional personnel.*

1. Program Manager - *Mandatory*

The Program Manager will provide consulting services to FCS management and technical staff and is responsible for solving complex contract and delivery issues and managing a series of projects under the scope of the task order. The Program Manager will serve as FCS's primary point-of-contact and will provide supervision and guidance for all contractor personnel assigned to the Task Order. The Program Manager is ultimately responsible for the quality, standards, and efficiency of the portfolio of services to include both technical issues and business processes. The Program Manager must be able to manage the base operations as well as the projected accelerated growth of the FCS program over the next five years.
Required Expertise:

- 15 or more years of IT experience, 10+ years providing program / project management for complex IT solutions
- Demonstrated experience in managing large scale programs of similar size, scope and complexity
- Proven ability to meet cost, schedule, and performance requirements for complex IT projects, or organizational transformation initiatives
- Excellent written and verbal communication skills, with proven results in coordinating and managing at the executive level
- BA or BS degree
- Project Management Professional (PMP) certified

Preferred Expertise:

- Masters level degree or Bachelor's level degree with equivalent work experience
- Relevant Agile Certification

2. Lead Cloud Architect- *Mandatory*

Develops the Current and Target State Architecture, Future Vision and migration path for the FCS products, services, and overall Ecosystem. Responsible for ensuring program increment (PI) objectives line up with the path to target state. Interfaces with senior clients, tenants, and technical staff to determine the recommended cloud strategy.
Required Expertise:

- 15+ years' experience in one or more architecture domains (e.g. business architecture, solutions architecture, application architecture)
- Advanced knowledge and experience in one or more current programming languages (E.g. - Java, Javascript (including AngularJS), Python, Rust, Go, Ruby or PHP)
- Experience in managing large operational cloud environments spanning multiple tenants through techniques such as Multi-Account management, AWS Well Architected Best Practices, OU/SCP, etc.
- Experience defining the architecture of cloud deployed applications
- Experienced with driving ongoing improvements in cost efficiencies such as purchase of Reserved Instance/Savings Plans aligned to resources consumption, review of AWS Trusted Advisor, etc.
- Expertise in service-oriented architecture, web services, and Application Programming Interfaces
- Experience with how containerized is performed with applications. Able to advise on the best forms of developing containerized application. (i.e., Docker, Rocket, etc.,)
- Experience with how container organization works and how the application needs to be Architecture to take advantage of that (Kubernetes, Universal Control Plane UCP, etc.,)
- Experience defining and driving SecDevOps best practices (e.g., IaC, CI/CD) within large teams
- Experience establishing legacy modernization and migration roadmaps for large scale applications
- Experience with event-driven applications using queues, service bus and other related patterns
- Exceptional verbal and written communication skills, and ability to work with minimal direction
- BA or BS degree in Science, Technology, Engineering, or Mathematics
- AWS Certified Solutions Architect – Professional Level

Preferred Expertise:

- Masters' Degree or Bachelor's level degree with equivalent years of work experience.
- Certified Kubernetes Administrator or other relevant Kubernetes Certification
- Relevant Agile Certification
- DOD IAM 3 or other relevant Security Certification

3. Senior Data Architect- *Mandatory*

This architecture role is a hands-on, leadership role combining technical expertise with

strategic vision and developing data architecture principles, standards, guidelines and concepts in a cloud environment at an enterprise scale. This position will also look at architectural strategies, design, and implementation for data governance, data management, data modeling, and data provisioning to meet enterprise requirements and objectives. Apply advanced consulting and extensive technical expertise to develop innovative solutions for data problems. Translate business requirements into technical solutions and develop the strategic data architecture.
Required Expertise:

- 10+ years' experience in developing strategies impacting the planning and delivery of IT services offered to internal clients, including Metadata and/or Master Data Management problems
- Data management, transformation, and migration experience using cloud native (e.g. AWS) data management pipelines, technologies and open-source tools
- Expertise recommending business intelligence and advance analytics tools in the federal market including Artificial Intelligence and Machine Learning capabilities
- Experienced with automating operations and workflow procedures for data transformations
- Strong background working in an agile development environment, collaborating with Application Development and Architecture Teams
- Expertise using Amazon Web Services (AWS) environment and databases like MySQL, PostgreSQL, Redshift etc.,
- Strong data management and transformation skills to provide efficient solutions and strong focus on business outcomes
- Expertise in big data architecture designing end-to-end solution on ingest, process, and analysis of large and complex data set
- Expertise in designing secure data layer as part of application or analytics environment
- Expertise to create logical data models for GSA FAS user community consumption
- BA or BS degree in Science, Technology, Engineering, or Mathematics

Preferred Expertise:

- Masters level degree or Bachelor’s level degree with equivalent work experiences
- Relevant Agile certification
- AWS Certified Solutions Architect – Associate Level
- AWS Certified Data Analytics – Specialty Level
- AWS Certified Machine Learning – Specialty Level

4. Senior Services Reliability Engineer- *Mandatory*

Manage, support and maintain a reliable environment for the site in order to ensure the stability and security of multiple systems/platforms that are run or operated in that environment. Develop or contribute to solutions to a variety of problems of moderate scope and complexity. Oversee the development of more robust systems for by building a resilient infrastructure. Build in redundancy, implement monitoring tools, and automate wherever possible and reduce toil by scripting routine tasks and automating self-repair.

Required Expertise:

- Experience in developing and managing Service Level Objectives (SLOs) for production systems
- Demonstrated experience in managing incident response teams (i.e., triaging, prioritizing and troubleshooting), detailing root cause analysis (RCAs), corrective actions and leading postmortems
- Experience in developing operational playbooks/runbooks, and disaster recovery testing
- Experience with reviewing system design and architecture documentation and preparing materials addressing security controls
- Experience working across product development teams to understand program goals
- Experience establishing or working with 'help desk' type ticket tracking and similar support processes
- Extensive experience with monitoring tools (e.g., Sysdig, New Relic, Twistlock, Splunk, etc.,) and understanding and expertise to automate alerting functions
- 3+ years of experience with Linux and Windows OS
- 2+ years of experience with DevOps/DevSecOps through CI/CD pipeline tools such as Jenkins
- 2+ years of experience with Jenkins and Github / Git / Gitflow
- 1+ year of experience with Docker and Containers
- 2+ years of experience with Agile development
- 2+ years of experience with Infrastructure as code: Terraform, Cloud Formation, Ansible, Packer
- 2+ year of experience with AWS services: EC2, RDS, Secrets Manager, IAM, etc.
- 2+ years of experience with troubleshooting applications and testing automation (e.g., Selenium)
- 1+ year of experience analyzing observability metrics, logs, traces
- BA or BS degree in Science, Technology, Engineering, or Mathematics
- AWS SysOps Administrator or AWS Developer – Associate Certificate

Preferred Expertise

- AWS Certified DevOps Engineer- Professional

5. Security Lead- *Mandatory*

The Security Lead will manage the FCS Division's Security Team and serve as the primary security point of contact for FCS. The lead will work with federal stakeholders to develop and implement strategy for advancing security operational compliance activities as part of a security framework aligned with the FCS vision. The Security Lead will provide management and coordination of security delivery for ongoing base operations as well as any investment initiatives that require security SME. The Security Lead will work closely with Product Owner to plan and prioritize operational compliance activities such as ATO recertifications, environment security posture and remediations, and security SRE. In addition, the Security Lead will identify improvements to regulatory security processes (e.g., TEP Component and Service Plans), tooling and security architecture input for new initiatives and products, as part of investment track.
Required Expertise:

- 15+ years establishing, managing and maturing security and compliance programs in federal and private sector focused on delivering complex Security IT solutions, resolving business challenges through technical implementation
- Experience in leading the analysis, assessment, design, and implementation of enterprise Cybersecurity solutions
- Experience in partnering with Business Leaders and Product Owners to influence and develop secure product visions and security informed roadmaps
- 10+ years of experience with risk management and development of mitigation strategies as well as coordinating strategies across multiple business lines, teams, and senior leadership.
- BA or BS degree in Cyber Security or related field
- DOD IAM 3 Security Certification

6. Security Compliance Engineer – *Optional*

Assist with the development, implementation, and administration of the FCS security program and systems ensure proprietary or confidential data and systems are protected by monitoring, auditing, and enforcing compliance with GSA and FCS Information Security and Information Technology policies, procedures, guidelines, and standards. The Security Compliance Engineer interfaces with clients to translate security and business requirements into technical design basis where security is the foundation to all decisions. Influences the design, configuration, implementation, and test and validation of complex security products, technology systems, services, and infrastructure with the aim of detecting security weakness prior to compromise, ensuring compliance with security standards and best practices.
Required Expertise:

- 7+ years of experience with reviewing system design and architecture documentation and preparing materials addressing security controls
- Experience with reviewing security scan results and determining the risk and impact of vulnerabilities
- Experience with Cloud security tools and processes, and coordinating with Product engineering
- Experience in establishing and implementing security activities (e.g., security compliance monitoring, networking, and engineering) as part of a DevSecOps environment in support of meeting cloud application and platform modernization requirements
- Experience in working with NIST and FISMA requirements and reporting
- Experience in implementing improvements to risk and threat barrier protections
- Experience in overseeing management of system vulnerabilities via Plan of Actions and Milestones
- 2+ years of experience with vulnerability scanning tool compliance and patch management to ensure compliance with Cybersecurity directives
- 1+ years of experience with Cybersecurity tools, including Netsparker, Fortify Webinspect, SonarQube, or Splunk
- CISA or Security+ certification preferred
- BA or BS degree in Engineering Technology, Computer Science, or a related

field

7. Information System Security Officer (ISSO) – *Optional*

Design, develop, and recommend integrated security system solutions that will ensure proprietary and confidential data and systems are protected. Provide technical engineering services for the support of integrated security systems and solutions. Interface with clients in the strategic design process to translate security and business requirements into technical designs. Configure and validate secure complex systems, tests security products and systems to detect security weaknesses.
Required Expertise:

- 10+ years of experience in managing complex regulatory and audit program, focusing on secured cloud capabilities, to include Authorization to Operate (ATO) in multi-tenant environment
- Experience working with the National Institute of Standards National Institute of Standards and Technology (NIST) and Federal Information Security Management Act (FISMA) requirements and reporting
- Experience in managing security Certification and Accreditation activities utilizing common control frameworks
- Experience with risk mitigation and selecting or designing appropriate security controls for implementation
- Experience applying cloud security concepts, requirements, design development, implementation, and integration for existing and new technology product offerings • Experience with overseeing compliance programs in Microsoft Azure, Amazon AWS, PCI DSS, and FedRamp cloud environments
- Experience in coordinating, monitoring and tracking security activities across multiple organizations
- Experience in managing security posture of cloud environment, and working with engineering teams to remediate, and communicating overall risk of environment while identifying areas of improvement
- Demonstrated understanding and experience with DevSecOps
- BA or BS degree in Science, Technology, Engineering, or Mathematics
- CISSP and/or CISA certification

8. Senior DevSecOps Engineer – *Optional*

Design, deploy, operate, and maintain secure Cloud products and services within a Cloud-based environment to enable development teams to deliver features in the most efficient way possible. Leverage an automated process to mitigate security vulnerabilities in the environment by working with the ISSO team to triage security vulnerabilities and planning mitigation activities, including but not limited to OS patching. Coordinate with a team of Cloud and DevOps engineers to help tenants realize value through product offerings and operations.
Required Expertise:

- The DevOps Engineer requires minimum of 10 years of programming experience o Includes 5+ years of experience in working within software engineer team who leveraged DevOps with development o Includes 5+ years of experience in at least two of the following fields in information security, computer or information science or related fields

- Experience using a wide variety of open source and COTS technologies and tools
- Experience in providing Analysis of Alternatives for tools and capabilities from various on premise, Cloud-based, and hybrid resources
- Experience in managing a Platform-as-a-Service environment (i.e., create blueprints, provision, maintain, upgrade and track inventory)
- Solid understanding of and experience implementing and integrating CI/CD Tools from the ground up, such as Atlassian (JIRA and Confluence), Github, Jenkins, Ansible, Artifactory, Docker, Kubernetes, Selenium, SonarQube, Gatling, JMeter, JUnit, AMP, aChecker, Jaws, Netsparker, OWASP ZAP, Tenable Nessus, Splunk, Prometheus, CloudWatch, New Relic, Grafana o Includes experience with Docker containerized application deployment and monitoring, cluster management
- Strong background working in an agile development environment, collaborating with Application Development and Architecture Teams
- Experience with service-oriented architecture, web services, Application Programming Interfaces
- Experience working in a High Availability environment with 99.99%+ uptime
- Strong background in Amazon Web Service (AWS), MySQL, PostgreSQL, MongoDB Apache, NGINX, PHP
- Comfortable writing deployment scripts in languages such as Python, Shell, AWS Cloud Formation, Groovy, and Golang
- Experience with systems and IT operations
- Comfort with automated, frequent, incremental code testing and deployment as part of a set of mature DevOps practices
- Strong grasp of automation tools (e.g., Cloudwatch, Lamdba, GitOps, Cloud Formation, etc.,)
- A strong focus on achieving value for business objectives
- Comfort with collaboration, open communication and reaching across functional borders
- Strong analytical, communication, and decision-making skills. Proficiency in a variety of computer programs and applications including VMWare, Windows, Linux, Oracle and Solaris.
- BA or BS degree in Science, Technology, Engineering, or Mathematics

9. Operations Lead - *Optional*

Drive quality control and assisting in delivering customer goals. Manage schedules, operational processes, and develop enhancements on current established processes. Track incidents and workflow using various tracking tools and collaborate with different workstreams to confirm all processes and procedures are followed. Communicate with client on the results of incident root cause analysis and identify gaps and improvements for operations and incident processes. Being process focused while managing client expectations.
Required Expertise:

- 12+ years of experience in quality management and process management
- Demonstrated experience managing similar size, scope and scale operations efforts
- Ability to analyze processes and identify gaps, resolutions and sharing

lessons learned
- 3+ years of experience with ServiceNow or similar ticketing tools
- 3+ years of experience with Jira or similar tools
- Excellent written and verbal communication skills
- Experience with Agile development methodologies and requirements gathering and analysis
- BA or BS degree in Science, Technology, Engineering, or Mathematics
- Relevant Agile certification

10. Product Portfolio Manager – *Optional*

Provide program direction to the implementation of a Product development methodology based on FCS Vision and Objectives, that delivers value to its customers and users. Coordinate product innovation and delivery across product teams and base operations through the alignment of internal structure and business processes, team structure and staffing. Work with Program Directors to provide recommendations on product roadmaps and enhancements with close coordination with Product Owners.
Required Expertise:
- 15+ of hands-on experience providing project management for complex IT solutions, focusing on resolving business challenges through technical implementation
- 10+ years of managing project scope and deliverables against available budget
- 10+ demonstrated experience in managing and implementing user-centric methodologies for the delivery of complex business challenges using a Product Development methodology across a portfolio of Products and Services
- 10+ years of experience in defining Digital Strategy in support of enterprise business objectives through implementation of Minimum Viable Products (MVP), managing Key Performance Indicators (KPIs), and establishing feedback mechanisms to mature product offerings
- 10+ years in partnering with Business Leaders and Product Owners to influence and develop Product Visions and Roadmaps informed by End-User feedback and experience
- 10+ years of experience with risk management and the development of mitigation strategies as well as coordinating strategies across multiple teams and senior leadership
- Proven ability to manage SecDevOps teams to achieve business value through technical delivery
- Excellent written and verbal communication skills
- Basic knowledge of AWS concepts and principals
- BA or BS degree in Science, Technology, Engineering, or Mathematics
- Masters' Degree preferred or Bachelor's level degree with equivalent years of work experience.
- Certification in Product Management
- Relevant Agile certification

11. Cloud Solutions Architect – *Optional*

Works closely with the Lead Architects to implement and drive secure, automated

solutions that are in alignment with the Target State architecture. Applies technology solutioning experience in order to provide implementation guidance based on best practices to the organization and tenants throughout the life cycle of the project.
Required Expertise:

- 10+ years of experience in designing and architecting large scale applications, including SaaS and cloud-based applications
- Ability to define and develop (code) infrastructure as code for a solution using organizational architectural design principles based on government FISMA and NIST requirements
- Experience in leading architecture sessions and provide implementation guidance based on existing design patterns of the organization throughout the life cycle of the project
- Experience in designing and open-source stack of trusted, high-performing Kubernetes solutions
- Extensive experience taking disparate business problems and delivering the best technology solutions for large scale applications
- Experience coordinating the evaluation, deployment, and management of current and future technology functionality for platform as a service across a major government organization
- Experience in designing, coding, and implementing next-generation enterprise CI/CD architecture using open-source tools and best practices
- Strong proficiency and understanding containers, container orchestration, auto-scaling, advanced deployment models, CI/CD with GitOps, and pipeline customization
- Expertise in service-oriented architecture, web services, and Application Programming Interfaces
- Experience in decomposing application components and determining how to leverage various technologies found with modern cloud services
- Experience working in one or multiple IT areas, but with the versatility to apply concepts for Cloud Enabled/Cloud native solutions, SecDevOps, Advanced Analytics, Machine Learning/Artificial Intelligence/RoboticProcess Automation, Integration/API/Microservices, User Experience
- Experience in applying Agile Methodologies e.g. Scrum, Kanban, SAFe, Lean
- BA or BS degree in Science, Technology, Engineering, or Mathematics
- Masters' Degree preferred or Bachelor's level degree with equivalent years of work experience

12. Agile Delivery Lead – *Optional*

Implement and improve Agile processes within a Product-focused organization, working closely with a team of Scrum Masters, Product Leads and Government Product Managers to ensure customer requirements are achieved via products and services. Manage Program Increment/Release and Sprint Planning – partner with product teams to plan for work based on priorities, facilitate planning sessions, and ensure teams are executing Agile best practices and ceremonies. Lead measuring and meeting Objectives and Key Results through development of key performance indicators for the portfolio of Cloud-based, open-sourced, Platform as a Service products and services. Communicate Risks and Issues, and Dependencies across teams by working closely with product delivery

teams and coordinating mitigation strategies and resolution. Work closely with governance board and ensure new feature requests that have been approved are routed appropriately to product teams for further decomposition, prioritization into backlogs, and alignment/impact to product backlogs. Perform regular backlog grooming sessions with product owners and technical leads to ensure development teams are well versed in functional expectations and delivery schedule

Required Expertise:

- 7+ years requirements gathering and synthesizing technical requirements, with 5+ years defining and implementing Agile best practices (i.e., SAFe, Agile ceremonies, LOE, etc.,)
- Demonstrated relevant experience performing this role on a program of similar size, scope, scale and complexity
- Foundational understanding of Product Management concepts (i.e., Product roadmaps, backlogs, KPIs, Definition of Done, Business Case Development).
- Demonstrated experience in facilitating large meetings, communication of vision to director-level audience, coordinating laterally across various teams.
- Proven ability to take complex features and break down into achievable epics, features and stories to achieve roadmap priorities.
- SAFe Release Train Engineer experience
- B.A. or B.S. Degree
- Certified Scrum Master
- Certified SAFe Agilist
- Certified SAFe Release Train Engineer

13. Cloud Advisory Lead – *Optional*

Provide oversight, strategic thought leadership, and innovative solutions towards maturing GSA IT-Wide cloud strategy, enablement, and shared service processes to include Cloud Advisory, Advocacy, Onboarding and Adoption, and Tenant self-service. Provide advisory services and technical expertise on increasing knowledge and accelerating cloud adoption for GSA stakeholders. Engage with tenants to understands business and technical priorities and challenges leading to requirements and help determine a targeted cloud strategy. Develop reusable tools to include enterprise cloud playbooks and standardized processes to increase awareness and reduce operational costs and timelines. Refine cloud economics model to continuously align investments to business value. Provide project management support and facilitate cross team coordination to develop and manage onboarding and adoption timelines and manage FCS activities required for major tenant deployments, to include identifying and managing associated risks, issues, and dependencies. Translate tenant specific milestones and key activities to program level cloud enablement roadmaps and presentations, tailored for both senior and executive level GSA leadership. Manage and enhance the processes required to triage, prioritize, and funnel tenant requests for new capabilities. Drive continuous improvement in areas that span requirements management, prioritization, service delivery, customer experience and engagement, organization change management, training, communications, performance measurement and management.

Required Expertise:

- 12+ years of demonstrated IT experience to include:
  - 8+ years of IT project management experience driving complex department and

agency level IT initiatives

- 6+ years of driving organizational change management activities for complex department and agency level IT initiatives,
- 6+ years managing customer experience, developing stakeholder engagement strategies and using data analytics to enrich experiences
- 6+ years driving process improvement leading to organizational efficiencies and reduction of operational costs
- 4+ years managing department level, to include developing enterprise cloud mission, vision and goals as well as organizational Key Performance Indicators (KPI)
  - Demonstrated experience leading Application Rationalization, IT Portfolio management and Cloud migration planning initiatives
  - Demonstrated experience de-composing work into a discrete set of milestones and associated set of risks, issues, and dependencies
  - Experience analyzing and reviewing IT investments and services to ensure they align with the business needs and strategy
  - Experience working with Service Now or Jira Service Desk, developing SLOs, and using data analytics to drive process improvement opportunities
  - Experience with SAFe and implementing Agile best practices, using Jira and Confluence to effectively plan and manage work
  - B.A. or B.S. Degree
  - Relevant Agile certification

6.4.2 Key Personnel Substitution

The Contractor shall not remove or replace any personnel designated as key personnel without making a written request to and receiving written concurrence from the Contracting Officer. Arbitrary moves are not acceptable and the contractor should plan on retaining key personnel for the life of the task order. The Government understands that personal circumstances and resignations of key personnel are out of the control of the Contractor. In such circumstances, qualified replacements should be sought expeditiously. Should key personnel need to be changed or replaced, the Contractor's request for a change to key personnel shall be made no later than ten (10) calendar days in advance of any proposed substitution and shall include a justification for the change. The request shall (1) indicate the labor category or labor categories affected by the proposed change, (2) include resume(s) of the proposed substitute in sufficient detail to allow the Government to assess their qualifications and experience, and (3) include a statement addressing the impact of the change on the Contractor performance. Requests for substitution will not be unreasonably withheld by the Government when valid reasons are provided, especially if the change will benefit the Government. The Government will approve initial contactor key personnel at time of award. Replacement key personnel will be approved via modification to the contract/task order. If the Government CO and the COR determine that the proposed substitution, or non-employee initiated removal of personnel without substitution or replacement, is unacceptable or would impair the successful performance of the work, the Contracting Officer will request corrective action. Should the Contractor fail to take necessary and timely corrective action, the Government may exercise its rights under the Disputes provisions of this contract or take other action as authorized under the provisions of this task order, the Prime contract upon which this order is based, or pursue other legal remedies allowable by law.

6.5 Personnel Retention and Recruitment

The contractor shall make every effort to retain personnel in order to ensure continuity until contract/order completion. If it should become necessary to substitute or replace personnel, the contractor shall immediately notify the COR and/or other identified Government representatives in writing of any potential vacancies and shall submit the resume(s) of replacement personnel within 5 calendar days of the notification. Additionally, for all new positions identified by the Government, the contractor shall submit the resume(s) of proposed personnel within 5 business days of the Government's initial request. The contractor shall submit the resume(s) of all potential personnel selected to perform under the contract/order to the COR and/or other identified Government representatives through GSA's web-based procurement system, or any other process means identified/required, for Government review and acceptance/rejection. Upon Government acceptance of a personnel resume(s), the candidate shall be available to begin performance within 14 business days. The contractor shall ensure continuity of operations during periods of personnel turnover and long-term absences. Long-term absences are considered those longer than one week in duration.

6.6 Non-Key Personnel Substitutions

Although Government approval is not required prior to replacing any of its non-key personnel staff, the Contractor shall provide resumes or other adequate documentation to verify to the Government that all proposed replacements (temporary or permanent) meet the security and minimum educational and experience requirements of this contract/order. Additionally, the Government requests the courtesy of being immediately informed of any potential vacancy or prior to any staff member being removed, rotated, re-assigned, diverted or replaced.

6.7 Staff Maintenance

The contractor shall make every effort to retain personnel in order to ensure work continuity until contract/order completion. During any periods of turnover or temporary absence of personnel, the Contractor shall ensure continuity of operations and make every effort to maintain manning without loss of service days to the Government. This may necessitate the use of temporarily assigned employees to fill short term gaps between permanently assigned employees or prolonged (more than one week) absences of current employees.

The Contractor is required to use and/or replace all personnel with those who meet the minimum qualifications as stipulated above, in this section of the PWS and should strive to replace departing personnel with those having appropriate and/or equal qualifications.Failure on the part of the Contractor to employ an adequate number of qualified personnel to perform this work will not excuse the Contractor from failure to perform required tasks within the cost, performance, and delivery parameters of this contract / order.

Due to the demanding nature of this program, it is essential that the Contractor maintain sufficient staffing levels to accomplish all required tasks. This is especially true because many labor skills are in short supply and the program must rely on a single employee to fill one or multiple roles.

6.8 Contractor Employee Work Credentials.

Contractors shall ensure their employees and those of their Subcontractors have the proper

credentials allowing them to work in the United States. Persons later found to be undocumented or illegal aliens will be remanded to the proper authorities.

7. GOVERNMENT FURNISHED PROPERTY/INFORMATION/ACCESS

7.1 General

The Government shall provide, without cost to the Contractor, the data, facilities, equipment, materials and services listed below. The Government furnished property and services provided as part of the contract/order shall be used only by the contractor and only to perform under this contract/order. No expectation of personal privacy or ownership using any Government electronic information or communication equipment shall be expected. All property at Government work sites, except for contractor personal items, will be assumed to be Government property unless an inventory of contractor property is submitted and approved by the CO/COR. Contractor personal items do not include government owned computers, external drives, software, printers, and/or other office equipment (e.g., chairs, desks, file cabinets). The contractor shall maintain an accurate inventory of Government furnished property.

7.2 Government Furnished items (Property)

7.2.1 Facilities

The Government will provide facilities at the authorized primary work locations asspecified in PWS paragraph 5.2. Use of the facilities by contractor personnel will includeall utilities, janitorial services and furniture for contractor personnel performing tasks. TheGovernment will provide the contractor access to buildings as required, subject to the contractor personnel obtaining the required clearances and approvals (See Section 8). Office space may include a private or shared cubicle, hoteling space (space reserved fortemporary use), or other such space suitable for the work, as required.

From time to time, as dictated by task requirements, contractors may be required to work at the GSA Headquarters. In those cases, the Government will provide access to tools to schedule workspaces/conference rooms.

NOTE: All Government-provided products and facilities remain the property of the Government and shall be returned upon completion of the support services. Contractor personnel supporting this requirement shall return all items that were used during the performance of these requirements by the end of the performance period.

7.2.2 Equipment and Network Access

The Government will provide the following at authorized on-site Government work locations subject to any required security approvals:

- A suitable work environment (i.e., telephone, office space and furniture). Office space may include a private or shared cubicle, hoteling space (space reserved for temporary use), or other such space suitable for the work required.
- A personal desktop computer or laptop and auxiliary hardware and software required in the performance of the contract/order.

- Network connectivity required to perform work assignments. Network and computer access rights commensurate with work assignments. NOTE: The Contractor shall immediately notify the COR who will terminate Government LAN access responsibility for any employee terminated or transferred from this contract.
- The Government will replace items that are determined to be beyond economical repair by the COR and/or other identified Government representatives unless damage or loss is determined to be due to contractor negligence.

7.2.3 Materials

Not applicable

7.2.4 Data

The Government will provide documents, reports, database access, data, and other information as available and as required to facilitate the accomplishment of work, as stated within this PWS.

The contractor is responsible for obtaining data necessary to perform each task if that data is in the public domain and is not otherwise furnished by the government.

Note: During the course of this task order, the Government may make additional Government Furnished Items (GFIs) -- materials, equipment, and facilities -- available upon receipt of a written request from the Contractor to the Government Technical Representative. These GFIs, if provided, would be in addition to those initially set forth above.

7.3 Use of Government Property (if applicable)

7.3.1 Soft Phones

Government soft phones may be provided as an application on Government provided computers. These are provided for use in conducting official business. Contractor personnel are permitted to make calls that are considered necessary and in the interest of the Government. The contractor shall follow the same policies as Government personnel for telephone usage.

7.3.2 Mobile/Wireless Telephones and Smart Devices

Government issued mobile/wireless telephone and smart devices may be assigned to contractor personnel when the Government determines it is in the Government's best interest. Contractor personnel are prohibited from using any Government issued device for personal use.

7.3.3 Electronic Mail (E-mail)

All Government e-mail access and use by contractor personnel shall be in support of the individual's official duties and contract/order responsibilities. All information that is created, transmitted, received, obtained, or accessed in any way or captured electronically using Government e-mail systems is the property of the Government.

Contractor personnel are prohibited from forwarding e-mail generated from a Government provided e-mail account to personal devices.

7.3.4 Copiers and Fax Machines

Copiers are to be used to copy material for official Government business only in the performance of the contract/order. Contractor personnel shall not use fax machines for other than official Government business in the performance of the tasks in the contract/order.

7.3.5 Computer and Internet

All Internet and electronic media access accomplished by contractor personnel (utilizing Government furnished equipment) shall be for official Government business in the performance of the tasks in the contract/order.

7.3.6 Canvassing, Soliciting, or Selling

Contractor personnel shall not engage in private activities for personal gain or any other unauthorized purpose while on Government-owned or leased property, nor may Government time or equipment be utilized for these purposes.

7.3.7 Security Violations Using Government Equipment

Any contractor violating Government security policies, guidelines, procedures, or requirements while using Government equipment or while accessing the Government network may, without notice, have their computer and network access terminated, be escorted from their work location, and have their physical access to their work location removed at the discretion of the CO/COR. The CO/COR will notify the contractor of the security violation and request immediate removal of the contractor employee.

NOTE: All Government-provided items remain the property of the Government and shall be returned upon completion of the support services. Contractor personnel supporting this requirement shall return all items issued to them when their performance on this contract/task order is ended.

7.4 Validation of Government Furnished Items (GFI) and Equipment Inventory

The contractor shall develop and maintain a complete GFI inventory that shall be made available to the Government upon request. Within three (3) business days of receipt of any GFI, the contractor shall validate the accuracy of the materials and notify the COR and/or other identified Government representatives, in writing, of any discrepancies, and update the GFI inventory list.

NOTE: Validation shall consist of the contractor checking for physical and logical completeness and accuracy. Physical completeness and accuracy shall be determined when all materials defined as Government furnished are provided. Logical completeness and accuracy shall be determined when all materials defined and associated with a program, system, or work package

are provided.

8. SECURITY

8.1 Non-Disclosure Statement.

Due to the potentially sensitive nature of the data and information associated with this requirement and with which contractor employees may work on a daily basis, all contractor personnel supporting this contract/order are required to complete the Government provided non-disclosure agreement/statement **(PWS Attachment C).** This statement shall be signed prior to assignment to the contract/order award to ensure information that is considered sensitive or proprietary is not compromised. Signed non-disclosure statements shall be provided to the COR and/or other identified Government representatives

The Contractor shall not release, publish, or disclose sensitive information to unauthorized personnel, and shall protect such information in accordance with provisions of the following laws and any other pertinent laws and regulations governing the confidentiality of sensitive information:

18 U.S.C. 641 (Criminal Code: Public Money, Property or Records)
18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information)
Public Law 96-511 (Paperwork Reduction Act)

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to Contractor employees while participating on this contract is considered proprietary.

8.2 Compliance with Security Requirements

Contractors entering into an agreement for services to the General Services Administration (GSA) and/or its Federal customers shall be contractually subject to all GSA and Federal IT Security standards, policies, and reporting requirements. The Contractor shall meet and comply with all GSA IT Security Policies and all applicable GSA and NIST standards and guidelines, other Government-wide laws and regulations for protection and security of Information Technology. There is no defined timeframe for the ATO, but the ATO must be approved and in place before any application/system can be deployed to production.

IT Security Procedural Guide: Security and Privacy Requirements for IT Acquisition Efforts CIO-IT Security-09-48, Section 2.4 states "The Contractor shall comply with Assessment and Authorization (A&A) requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization."

All data shall be encrypted in transmission and at rest.

The Contractor shall be responsible for ensuring all strategic planning, technical implementations and operations take into account necessary requirements resulting from the Executive Order on Improving the Nation's Cybersecurity (EO 14028, May 12, 2021).

The Contractor shall be responsible for ensuring all employees supporting this contract

comply with all security requirements imposed by the Government Security Officer at all times while in Government facilities and shall follow the instructions of the local organization pertaining to security.

The Federal Information Security Modernization Act (FISMA) of 2014 provides a comprehensive framework for ensuring the effectiveness of information security controls across Federal agencies. FISMA focuses on the program management, implementation, and evaluation aspects of the security of federal information systems. It codifies existing security policies, including Office of Management and Budget (OMB) Circular A-130, Revised, and reiterates security responsibilities provided for in the Computer Security Act of1987, the Paperwork Reduction Act (PRA) of 1995, and the Clinger-Cohen Act (CCA) of 1996.

In order to protect against cybersecurity threats and manage GSA information systems, the Vendor shall ensure that the contract is compliant with Federal security standards and GSA requirements. The Vendor must provide security and protection for information systems that support the operations and assets of the agency, including the support activities provided or managed by a contractor. Relevant areas that GSA's policies address include:

- Security Requirements
- Cloud information system
- Mobile application
- Privacy Protection
- Controlled Unclassified Information
- Incident Reporting Requirements
- Software License Management
- Telecommunications Policy
- Social Media Policy

The Contractor and subcontractors must insert the substance of this section in all subcontracts.

8.3 IT Security Requirements

Contractors are required to comply with Federal Information Processing Standards (FIPS), the "Special Publications 800 series" guidelines published by NIST. Federal Information Processing Standards (FIPS) publication requirements are mandatory for use. NIST Special Publications are guidance unless required by GSA Chief Information Security Officer and/or GSA policies, procedures or procedural guides, in which case usage is mandatory. In addition, Contractors are required to comply with GSA Acquisition Letter MV-19-04.

- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems" http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems" http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
- FIPS PUB 140-2, "Security Requirements for Cryptographic Modules"

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

- NIST Special Publication 800-18 Revision 1, “Guide for Developing Security Plans for Federal Information Systems” http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf
- NIST Special Publication 800-30 Revision 1, “Guide for Conducting Risk Assessments” http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- NIST Special Publication 800-34 Revision 1, “Contingency Planning Guide for Federal Information Systems”http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
- NIST Special Publication 800-37 Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach” http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
- NIST Special Publication 800-47, “Security Guide for Interconnecting Information Technology Systems” http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf
- NIST Special Publication 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations” http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- NIST Special Publication 800-53A Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans” http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

8.4 Safeguarding Sensitive Data and Information Technology Resources

The contractor may have access to sensitive (to include privileged and confidential) data, information, and materials of the United States (U.S.) Government. These printed and electronic documents are for internal use only and remain the sole property of the U.S. Government. Some of these materials are protected by the Privacy Act of 1974 (AMENDED) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

The Contractor shall be responsible for ensuring all strategic planning, technical implementations and operations take into account necessary requirements resulting from the OMB Memo Evidence-Based Policymaking: Learning Agendas and Annual Evaluation Plans (OMB Directive M 21-27, June 30, 2021).

A. In accordance with FAR 39.105, this section is included in the contract.
B. This section applies to all who access or use GSA information technology (IT) resources or sensitive data, including awardees, Contractors, subcontractors, lessors, suppliers and manufacturers.
C. The GSA policies as identified in paragraphs of this section are applicable to the contract. These policies can be found at http://www.gsa.gov/directives or

https://insite.gsa.gov/directives. All the GSA policies listed in this paragraph must be followed.

a. CIO P 1878.2A Conducting Privacy Impact Assessments (PIAs) in GSA
b. CIO P 2100.1 GSA Information Technology (IT) Security Policy
c. CIO P 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
d. CIO 9297.1 GSA Data Release Policy
e. CIO 9297.2B GSA Information Breach Notification Policy
f. CIO P 2100.2A GSA Wireless Local Area Network (LAN) Security
g. CIO 2100.3C Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities
h. CIO 2104.1A GSA Information Technology IT General Rules of Behavior
i. CIO 2182.2 Mandatory Use of Personal Identity Verification (PIV) Credentials
j. ADM P 9732.1 D Suitability and Personnel Security
k. CIO 2102.1 Information Technology (IT) Integration Policy
l. CIO 2105.1 C GSA Section 508: Managing Electronic and Information Technology for Individuals with Disabilities
m. CIO 2106.1 GSA Social Media Policy
n. CIO 2107.1 Implementation of the Online Resource Reservation Software
o. CIO 2108.1 Software License Management
p. CIO 2160.29 GSA Electronic Messaging and Related Services
q. CIO 2160.4A CIO Provisioning of Information Technology (IT) Devices
r. CIO 2162.1 Digital Signatures
s. CIO P 2165.2 GSA Telecommunications Policy
t. CIO IL-13-01 Mobile Devices and Applications
u. CIO IL-14-03 Information Technology (IT) Integration Policy
v. HCO 9297.1 GSA Data Release Policy
w. HCO 9297.2B GSA Information Breach Notification Policy
x. ADM P 9732.1 D Suitability and Personnel Security
y. (i) CIO 09-48, IT Security Procedural Guide: Security and Privacy IT Acquisition Requirements
z. (ii) CIO 12-2018, IT Policy Requirements Guide

This section shall be inserted in all subcontracts.

8.5 Employee Security Requirements

The contractor shall provide personnel who already have or are capable of attaining and maintaining a Tier 2S security fitness determination. Employees who undergo a Tier 2S Investigation (formerly called Moderate Risk Background) and must have a favorable outcome after the investigation and adjudication in order to work on the contract. No access will be given to the Government computer information systems and Government sensitive information before the background investigation is completed. When Government on-site meetings are required, the Government will provide personnel to ensure approved contractor personnel have access to Government facilities. Selected contractor employees will be

required to complete mandatory Security Awareness and Privacy Training (this training is often provided internally by GSA via GSA Online University).

8.5.1 New Contractor Personnel

The full names of all contractor personnel proposed to work under this contract must be submitted to the COR and GSA Security for initiation and/or verification of an individual's security clearance investigation status. No work shall commence under the contract until GSA has received either an initial Enter On Duty notification (EOD) or a final favorable adjudication and have been approved to work on the contract.

8.5.2 Departing Contractor Personnel

The Contractor shall notify the COR, Contracting Officer and the GSA Personnel Security Officer when Contractor personnel will no longer be working on the contract. The Contractor must then turn in all badges; Government furnished equipment, and deliverables and provide an updated listing of GFE.

8.6 Common Access Card & ID Badges

When Government facilities are utilized in performance of this contract, the Government will provide photo identification, such as Common Access Card (CAC) and Restricted Area Badge (as required). The Contractor shall comply with all requirements necessary to obtain a CAC and Restricted Area Badge. Once issued, these credentials will allow Contractor employees unescorted entry into Government facilities.

8.7 Facility Security Requirements – (Not Applicable)

8.8 Personal Identity Verification

The Contractor shall comply with the following Personal Identity Verification clause.

52.204-9, Personal Identity Verification of Contractor Personnel. (Jan 2006)
(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201.
(b) The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally-controlled facility or access to a Federal information system.

End of Clause

9. SPECIAL INSTRUCTIONS

9.1 Contractor Performance Assessment Reporting System (CPARS) Assessment

Upon request by the Government, the contractor shall submit a self-evaluation of their performance at least annually utilizing a Government provided template. From time of Government request, the contractor shall have 7 business days to provide input to the GSA COR. The contractor self-assessment will then be submitted to the Government client where they will utilize this information to formulate an independent performance evaluation that will be processed through the Contractor Performance Assessment Reporting System. The requirements of the FAR and its supplements as it pertains to CPARS reporting shall be adhered to.

9.2 Personal Services

This is not a "Personal Services" contract as defined by FAR 37.104. The government has taken the following steps and precautions to ensure that "Personal Services" employer-employee relationships are not created between government and contractor employees during performance of this task order. Although Contractor employees who furnish services under this contract are subject to Government technical oversight, neither the Government nor a Government authorized third party contractor or representative shall oversee Contractor employees but shall provide all direction through the Contractor's designated representative(s) who is/are solely responsible for supervising and managing Contractor employees. In further compliance with this regulation –

- All tasks will be initiated using approved Task Directive Forms or other approved form of documentation.
- All government direction or approval of contractor-initiated suggestions shall be documented using approved Task Directive Forms or other approved form of documentation
- All government contract monitors shall communicate with the contractor through the approved contractor management representative.
- All government representatives responsible for managing this task order shall be briefed on the avoidance of personal services and those actions that represent personal services, prior to assuming their contract responsibilities.

9.3 Privacy Act

Work on this project may require that contractor personnel have access to information which is subject to the Privacy Act of 1974. Personnel shall adhere to the Privacy act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations when handling this information. Privacy Act information is considered sensitive and appropriate safeguards shall be implemented by the contractor. The contractor is responsible for ensuring all contractor personnel are briefed on privacy Act requirements.

9.4 Rehabilitation Act Compliance (Section 508)

Unless otherwise exempt, all services and/or products provided in response to this requirement shall comply with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR part 1194).

The Contractor shall support the Government in its compliance with Section 508 throughout the development and implementation of the work to be performed. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burdenwould be imposed on the agency.

Additional information regarding Section 508 can be obtained from the following web sites.

http://www.section508.gov/index.cfm?FuseAction=Content&ID=12
http://www.access-board.gov/508.htm
http://www.w3.org/WAI/Resources

9.5 Final Invoice and Release of Claims

The contractor is required as a deliverable of the contract/order to provide a final invoice no later than 30 calendar days after the end of the period of performance. Additionally, the contractor shall provide a Release of Claims no later than 90 calendar days after the end of the period of performance. The contract/order will be modified for closeout.

9.6 Other Direct Costs (ODCs)

The Government may require the contractor to purchase materials and equipment and ODCs, to include hardware, software, and related supplies critical and related to the services being acquired under the contract/order. Such requirements will be identified at the time the contract/order is issued or may be identified during the course of a contract/order by the Government or the contractor. Prior to initiating a purchase, the contractor shall obtain Government approval of the item(s) to be purchased from the GSA COR by submitting a **Request to Initiate Purchase (RIP)** (**Form determined after award**). Once approved, the contractor may initiate the purchase action. If the contractor initiates a purchase within the scope of the contract/order and the prime contractor has an approved purchasing system, the contractor shall execute the purchase and provide a copy of the purchase order to the GSA COR. If the prime contractor does not have an approved purchasing system, the contractor shall submit a **Consent to Purchase (CTP)** (**Form determined after award**) to the Contracting Officer to verify that the purchase was carried out according to appropriate regulations. The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the GSA COR or, if required, an approved CTP from the CO. On a case-by-case basis, the CO may require the contractor to submit a CTP even if the contractor has an approved purchasing system.

9.7 Avoidance and/or Mitigation of Actual or Potential Organizational Conflicts of Interest

Contractor employees may have access to sensitive government information while

performing this work, may be involved in reviewing and assessing the work of other contractors, and may be involved in developing specifications and work statements for subsequent or complementary work. There is a potential for organizational conflicts of interest if the Contractor has ties with firms whose work it will review or if the Contractor is subsequently awarded a contract that uses a specification or work statement that it prepared. To avoid actual or potential organizational conflicts of interest, the Contractor, in conjunction with Government scheduling and oversight controls, must be able to mitigate its relationship with a firm whose work it might review during performance of this Task Order. No specific firm is currently identified but firm may be identified during the course of contract/task order performance. Additionally, the Contractor shall refrain from seeking contracts that incorporate Contractor generated specifications or work statements until it first demonstrates, to the satisfaction of the Contracting Officer, that obtaining such other contracts will not create an actual or potential organizational conflict of interest with work performed on this task order. The Contractor shall comply with the provisions of the task order clauses entitled “Organizational Conflicts of Interest,” “Notification of Conflicts of Interest Regarding Personnel,” “Limitation of Future Contracting,” and “Annual Conflict of Interest Certification” to meet this requirement, which shall be incorporated into the Task Order.

9.8 Task Order Management

9.8.1 Contracting Officer’s Representative (COR)

The Government Contracting Officer is primarily responsible for managing this contract / order. Additionally, the work to be performed under this contract / order is subject to monitoring by an assigned Contracting Officer’s Representative (COR). The COR appointment letter, outlining the COR responsibilities under this contract/order, will be provided to the contractor under separate cover. Questions concerning COR appointments should be addressed to the Contracting Officer.

9.8.2 Government Technical Representative – Task Management

In addition to the COR, the Government may assign one or more Technical Representatives [Technical Point of Contacts (TPOC)]to monitor the technical aspects of this contract / order. The Government Technical Representative will participate in project meetings and review and acceptance of task order deliverables and will otherwise provide the COR with technical assistance and clarification required for contract / order performance. Refer to the attached QASP for specific information on project monitoring.

9.9 Technical Direction

All work shall be performed within the scope of this PWS and the Government will not ask or require the Contractor to perform work that is outside of the scope of this Contract/Task Order. Clarification to the work may be provided to the Contractor in writing by the Contracting Officer’s Representative (COR) using a Technical Directive form or other agreed upon written documentation. The Contractor’s representative shall acknowledge receipt of such technical direction in writing. If specific tasks that fall within the scope of the performance objectives of this PWS are requested, amplified, or clarified by written technical direction, the Contractor shall comply with that direction, which shall become a part of this task order. Technical direction shall be provided at the management level and Contractor employees shall perform work as specified in this Contract/Task Order as directed by the

Contractor's designated project manager, who shall have full responsibility for the assignment and monitoring of Contractor employee activities.

Task directives may include deliverables that are not initially identified in this task order. If so, task directives shall include specific delivery dates and places for reports and studies or a specific completion date for support services. As an alternative, the task directives may require the Contractor to establish timelines and milestones for completion of tasks. Government specified delivery or completion dates and Government approval of Contractor proposed timelines or milestones shall be binding on the Contractor.

Technical direction does not change the total dollar value of the contract or order; however, the dollar value of specific work identified in the technical directive may be obtained from the contractor for administrative purposes (e.g. proper allocation of funds, payment of invoices).

If the Contractor believes that any technical direction requires performance of work that is outside the scope of this contract / order, the Contractor shall immediately contact the Contracting Officer.

If specified in any technical direction document, the Contractor shall start work described in each Task Directive ONLY after receiving a written Government authorization to proceed. Otherwise, the Contractor can start work as soon as the technical direction is given.

9.10 Data Ownership/Release/Availability/Rights

All Government data collected in the system is the property of the Federal Government. All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period in an electronic open standard data format that is easily reusable. The data shall be provided to the Government at no additional cost. The Government shall be afforded 14 calendar days to verify and validate the data and the Contractor shall be required to correct performance if errors or omissions are found.

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for the protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

The Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the Cloud Services or to provide the Cloud Services to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other

legal requirement, the Contractor will give Government reasonable notice of any such legal requirement or order, to allow Government to seek a protective order or other appropriate remedy.

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor and shall not be used for any other purpose other than that specified herein. The Contractor shall provide requested data at no additional cost to the government.

The Government will retain unrestricted rights to government data. GSA must own and control its data, interfaces, processes, business rules and information with the ability to export easily and readily to other applications/systems/ Contractors in readable, usable formats, without added investments as the need arises. GSA retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request copies of these at any time.

9.11 Data Rights

The Government shall have unlimited royalty free rights to all data originally developed, generated and delivered under this contract or order as prescribed by the clause entitled **Rights in Data—General** (FAR 52.227-14**)** which is incorporated into this task order or into the indefinite quantity contract upon which this order is based. The Contractor shall retain all rights to data used to meet the requirements of this task order if developed solely at the Contractor's expense for their commercial applications and sales.

The Government shall have the right to use all commercially developed and privately funded data delivered under this contract or order in accordance with, and subject to, the published agreements and restrictions that accompany that data.

9.12 Limited Use of Data

All data delivered or made available to the Contractor as Government Furnished Data shall remain the property of the Government and shall only be used by the Contractor in the performance of this contract or order. The Government retains all rights to Government Furnished Data.

At the conclusion of this contract/order all Government Furnished Data shall be dealt with according to the disposition instruction provided by the Contracting Office. If the Contracting Officer fails to provide disposition instruction for Government Furnished Data within thirty days of contract/task order end, the Contractor shall return all hard copy data and delete or otherwise destroy all electronic data.

9.13 Proprietary Data

The Contractor shall not employ the use of any proprietary data or software in the performance of this contract without the advanced written consent of the Contracting Officer.

9.14 Inspection and Acceptance

Inspection and acceptance will occur in accordance with the clause entitled Inspection of Services – Time and Material and Labor Hour (FAR 52.246-6).

Payment for the correction of defective or deficient work will be handled as follow:

The Contractor will not be paid profit associated with re-performance of any defective or deficient time and material or labor hour work per the clause FAR 52-246-6 (f) Inspection-T&M.

In the absence of other agreements negotiated with respect to time provided for government review or specifically stated in other parts of this PWS, deliverables will be inspected and the contractor notified of the Government's Technical Representative's findings within five (5) workdays of normally scheduled review. Unacceptable or unsatisfactory work will be handled as outlined in the QASP. Acceptance of invoices shall constitute acceptance of performance.

Inspection and acceptance shall be at destination.

9.15 Contract Type

This contract / order will be awarded using a Time and Material contract type.

9.16 Ceiling Price Notification

Per clause 52.323-7, Payments under Time-and-Materials and Labor-Hour Contracts, the contractor is reminded – "If at any time the Contractor has reason to believe that the hourly rate payments and travel costs that will accrue in performing this contract in the next succeeding 30 days, if added to all other payments and costs previously accrued, will exceed 85 percent of the ceiling price in the Schedule, the Contractor shall notify the Contracting Officer giving a revised estimate of the total price to the Government for performing this contract with supporting reasons and documentation."

9.17 Task Order Funding

It is anticipated that the task order will be incrementally funded. Accordingly, the following provision applies.

Incremental Funding

(GSA 5QZA AOD Memo, Subject: Incremental Funding-3 2009 01 (revised 07-23-09)

This project may be incrementally funded. If incrementally funded, funds will be added to this task via a unilateral modification as they become available. Contractor shall not perform work resulting in charges to the government that exceed obligated funds.

The Contractor shall notify the Contracting Officer in writing, whenever it has reason to believe that in the next 60 days, when added to all costs previously incurred, will exceed 75% of the total amount so far allotted to the contract/order by the Government. The notice shall state the estimated amount of additional funds required to complete performance of the contract/order for the specified period of performance or completion of that task.

Sixty days before the end of the period specified in the Schedule, the Contractor shall

notify the Contracting Officer in writing of the estimated amount of additional funds, if any, required to continue timely performance under the contract/order or for any further period specified in the Schedule or otherwise agreed upon, and when the funds will be required.

The government is not obligated to reimburse the Contractor for charges in excess of the obligated funds and the Contractor is not obligated to continue performance or otherwise incur costs that would result in charges to the government in excess of the amount obligated under this order.

End of clause

9.18 Material and Material Handling Costs (not applicable)

9.19 Productive Direct Labor Hours

The Contractor shall only charge for labor hours when work is actually being performed in connection with this Task Order and not for employees in a "ready" status only. For this task order 1 FTE (full time equivalent) = 1920 labor hours.

9.20 Invoicing and Payment

Payments will be made in accordance with the clause entitled Payments (FAR 52.232-1) or Payments under Time-and-Materials and Labor-Hour Contracts (FAR 52.232-7).

The Contractor may invoice for items upon their delivery or services when rendered. Billing and payment shall be accomplished in accordance with contract terms and GSA payment procedures. Invoice submission instructions shall be provided at the time of award.

9.21 Payment for Unauthorized Work

The Contractor will not be paid for the performance of work that is not authorized under this Task Order. No payments will be made for any unauthorized supplies and/or services or for any unauthorized changes to the work specified herein. This includes any services performed by the Contractor on their own volition or at the request of an individual other than a duly appointed CO, COTR, or Government Technical Representative. Only a duly appointed CO is authorized to change the specifications, terms, or conditions under this effort

10 ATTACHMENTS

Attachment A - Cloud Service Appendix

Tab A - Key Personnel

Tab B - Total Tenants

Tab C - Licensing

Tab D - Products & Services

Tab E - FY22 Program OKR's

Tab F - Data ProSrv

Tab G - Tenant Invoice

Tab H - Performance Measures

Tab J - Deliverables

Tab K - Terms & Jargon

Tab L - Standard Operating Procedures

Tab M - Technology Inventory

Attachment B – QASP (Quality Assurance Surveillance Plan)

Attachment C – Non-Disclosure Agreement